

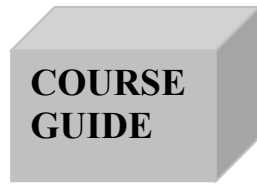


NATIONAL OPEN UNIVERSITY OF NIGERIA

SCHOOL OF BUSINESS AND HUMAN RESOURCE  
MANAGEMENT

COURSE CODE:MBA 754

COURSE TITLE:FRAUD DETECTION AND ELECTRONIC  
BANKING



**MBA 754**

**FRAUD DETECTION AND ELECTRONIC BANKING**

Course Developer/Writer

Gerald C. Okereke

National Open University of Nigeria

Programme Leader

Dr. O.J. Onwe

National Open University of Nigeria

Course Coordinator

Abdullahi .S. Araga

National Open University of Nigeria



**NATIONAL OPEN UNIVERSITY OF NIGERIA**

National Open University of Nigeria  
Headquarters  
14/16 Ahmadu Bello Way  
Victoria Island  
Lagos

Abuja Office  
No 5 Dar es Salam Street  
Off Aminu Kano Crescent  
Wuse II, Abuja  
Nigeria.

e-mail: [centralinfo@nou.edu.ng](mailto:centralinfo@nou.edu.ng)  
URL: [www.nou.edu.ng](http://www.nou.edu.ng)

Published by  
National Open University of Nigeria

Printed 2009

ISBN: 978-059-619-9

All Rights Reserved

<b>CONTENTS</b>	<b>PAGE</b>
Course Aims.....	1
Course Objectives.....	1
Study Units.....	2
Assessment .....	2

### **Course Aims**

This course is designed to acquaint students, information technology managers and financial managers of interplay between fraud and electronic banking. It is aimed at extensive examination of the forms of electronic fraud that plague financial transactions, and in so doing

explore ways to dealing with electronic fraud. The nature and forms of electronic banking is also examined with the intension to compare and contrast forms of electronic banking. Through a thorough x-ray of how to deal with electronic fraud schemes, we inspire confidence in would be electronic fund managers and investors to engage in electronic banking transactions.

## **Course Objectives**

At the end of this course you should be able to:

- Explain electronic banking and the relationship it has with e-commerce
- Thoroughly explain the services offered customers in e-banking transactions
- Answer the question of the challenges facing forms of e-banking
- Give an account of the characteristics of Internet banking
- Explain Internet fraud and its origin
- Explain how to identify some the Internet fraud schemes
- Define advance fee fraud and explain its origin
- Answer the question of how 419 is implemented
- Differentiate advance fee fraud from credit card and Forex frauds
- Identify some agency warnings that concern Forex business
- Enumerate the steps in strategic fraud detection
- Explain the different types of electronic fraud detection techniques
- Identify future trends in the development of electronic fraud detection techniques
- Explain the preliminary procedure of conducting an electronic/Internet banking audit
- Show how to deal with legal and regulatory matters in the Internet auditing process.
- State the types of risks associated with computerised electronic banking system
- Identify areas in which computerisation in electronic banking can lead to detection and prevention of fraud
- Explain what biometrics is and why biometrics is deployed in fraud detection and prevention schemes
- State the issues and challenges facing biometrics and its applications in fraud prevention and detection
- Explain how some governments and organisations have also used artificial intelligence and biometrics to check fraud
- Answer the question of risk factors associated with fraud schemes
- Expressly state how to deal with fraud in organisations.

## **Study Units**

The study units of this course are:

### **Module 1**

Unit 1	Introduction to Electronic Banking
Unit 2	Introduction to E-Banking (2): Types of Electronic Banking
Unit 3	Information Systems Auditing For Internet Banking
Unit 4	Electronic Fraud (1) Internet Fraud
Unit 5	Electronic Fraud (2) Advance Fee Fraud

### **Module 2**

Unit 1	Electronic Fraud (3) Credit Card Fraud and Forex Scam
Unit 2	Strategic Fraud Detection
Unit 3	Electronic Fraud Detection Techniques
Unit 4	Control and Auditing Of Information System
Unit 5	Guidelines For Electronic/Internet Banking Audit Program

### **Module 3**

Unit 1	Risks and Security in Electronic Banking
Unit 2	Introduction to Biometrics
Unit 3	Application of Biometrics and Artificial Intelligence (AI) in Electronic Fraud Detection
Unit 4	Identifying and Responding to Electronic Fraud Risks: <i>The Case of Australia</i>

### **Assessment**

The assignments represent 30% of the marks obtainable.

Examination constitutes 70% of the marks obtainable.

Course Code	MBA 754
Course Title	Fraud Detection and Electronic Banking
Course Developer/Writer	Gerald C. Okereke National Open University of Nigeria
Programme Leader	Dr. O.J. Onwe National Open University of Nigeria
Course Coordinator	Abdullahi .S. Araga National Open University of Nigeria



## **NATIONAL OPEN UNIVERSITY OF NIGERIA**

National Open University of Nigeria  
Headquarters  
14/16 Ahmadu Bello Way  
Victoria Island  
Lagos

Abuja Office  
No 5 Dar es Salam Street  
Off Aminu Kano Crescent  
Wuse II, Abuja  
Nigeria.

e-mail: [centralinfo@nou.edu.ng](mailto:centralinfo@nou.edu.ng)  
URL: [www.nou.edu.ng](http://www.nou.edu.ng)

Published by  
National Open University of Nigeria

Printed 2009

ISBN: 978-059-619-9

All Rights Reserved



<b>CONTENTS</b>	<b>PAGE</b>
<b>Module 1</b> .....	<b>1</b>
Unit 1 Introduction to Electronic Banking.....	1
Unit 2 Introduction to E-Banking (2): Types of Electronic Banking.....	15
Unit 3 Information Systems Auditing for Internet Banking.....	33
Unit 4 Electronic Fraud (1) Internet Fraud .....	50
Unit 5 Electronic Fraud (2) Advance Fee Fraud.....	63
<b>Module 2</b> .....	<b>79</b>
Unit 1 Electronic Fraud (3) Credit Card Fraud and Forex Scam .....	79
Unit 2 Strategic Fraud Detection.....	92
Unit 3 Electronic Fraud Detection Techniques.....	109
Unit 4 Control and Auditing Of Information System.....	124
Unit 5 Guidelines For Electronic/Internet Banking Audit Programme.....	138
<b>Module 3</b> .....	<b>154</b>
Unit 1 Risks and Security in Electronic Banking.....	154
Unit 2 Introduction to Biometrics.....	172
Unit 3 Application of Biometrics and Artificial Intelligence (AI) in Electronic Fraud Detection.....	188
Unit 4 Identifying and Responding to Electronic Fraud Risks: The Case of Australia.....	202



**MODULE 1**

Unit 1	Introduction to Electronic Banking
Unit 2	Introduction to E-Banking (2): Types of Electronic Banking
Unit 3	Information Systems Auditing For Internet Banking
Unit 4	Electronic Fraud (1) Internet Fraud
Unit 5	Electronic Fraud (2) Advance Fee Fraud

**UNIT 1 INTRODUCTION TO ELECTRONIC BANKING****CONTENTS**

1.0	Introduction
2.0	Objectives
3.0	Main Content
3.1	What is Electronic Banking?
3.2	Organisation's/Client's View about Electronic Banking
3.2.1	Electronic Banking Services
3.3	What are the Advantages and Potential Difficulties of Electronic Banking?
3.4	Is Electronic Banking as Secure as More Traditional Methods of Banking?
3.5	People's Opinion
3.6	Other Concerns about Electronic Banking
3.7	Benefits of Online Banking: Case Study of Washington Mutual Bank
4.0	Conclusion
5.0	Summary
6.0	Tutor-Marked Assignment
7.0	References/Further Readings

**1.0 INTRODUCTION**

After the invention of paper, most organisations including government organisations and banks march on paper. Nevertheless, as information technology evolves, the new technology has to play a part in helping the process of organisations. Information technology, particularly the healthy synergy of computers and communications has practically affected every sector of the economy covering the entire spectrum of manufacturing products and services. Banking is no exception to this pervasive impact of IT.

We are living in an era where certain important developments are taking place. The first is the extensive use of information technology in

banking and all financial services. The world has become a global village, thanks to advances in telecommunication. In this era of globalisation, billions of dollars can be moved from one part of world to another at the touch of a computer mouse, at the speed of light. Information technology is totally changing the banking business. In fact, Thomas D. Steiner and Diogo B. Teixeira in their book *Technology in Banking* have characterised the whole development as creating value, destroying profits – technology is creating value for the customer but destroying the profits for the banks.

As technology creates value for the customer, it is also destroying profits for the service providers like the banks. Does this mean that the banks can ignore technology? The choice before the banks is between annihilation by not adopting technology and bankruptcy because of the extreme competition and lowering profit margins.

Another important aspect of banking is that it is also like many other industries getting unbundled. The authors of *Technology in Banking* point out that banking is very far from being a homogenous activity. In fact it is a collection of more than 150 specific products / market services. Lines of business differ by customer whether retail, corporate or other financial institutions. They differ by distribution channel, whether by branch, by direct salesman or by mail. They differ by product route, whether lending, deposit gathering or payment product.

The overall strategy for the bankers and financial institutions in using information technology are:

- Link business strategy more effectively with technological reality
- Adopt simultaneous tight-loose policies to manage systems investments
- Treat routine automation differently from distinctive automation
- Consider industry systems capacity when making product decisions
- Focus, focus, focus: Get rid of those huge shared cost structures.

## **2.0 OBJECTIVES**

At the end of this unit, you should be able to:

- explain what electronic banking is and the relationship it has with e-commerce
- identify the services offered to customers in e-banking transactions
- state the advantages and disadvantages of electronic banking
- explain what people feel about e-banking
- establish how secure e-banking is.

## **3.0 MAIN CONTENT**

### **3.1 What is Electronic Banking?**

For many consumers, electronic banking means 24-hour access to cash through an Automated Teller Machine (ATM) or Direct Deposit (DD) of paychecks into checking or savings accounts. But electronic banking now involves many different types of transactions.

Electronic banking, also known as Electronic Fund Transfer (EFT), uses computer and electronic technology as a substitute for checks and other paper transactions. EFTs are initiated through devices like cards or codes that let you, or those you authorise, access your account. Many financial institutions use ATM or debit cards and Personal Identification Numbers (PINs) for this purpose. Some use other forms of debit cards such as those that require, at the most, your signature or a scan.

The term “electronic banking” or “e-banking” covers both computer and telephone banking. Using computer banking, an organisation’s or client’s computer either dials directly into its bank’s computer or gains access to the bank’s computer over the Internet. Using telephone banking, the charity controls its bank accounts by giving the bank instructions over the telephone. Both computer and telephone banking involve the use of passwords, which give access to the charity’s accounts.

Using these methods, banking transactions can be actioned 24 hours a day. Computer banking allows an organisation or individual, for instance, to view recent transactions, print out statements and transfer funds between accounts and make payments. Many banks also have the facility for a charity to set up, amend or cancel standing orders. Electronic banking also allows payments to be made to the charity, i.e. acceptance of credit card donations. Most organisations or individuals that use electronic banking will also continue to use some of the elements of more traditional methods of banking, such as a cheque-book.

Electronic banking services differ between the different banks and building societies. If trustees decide that they want to use electronic banking then they should shop around for the most suitable package for their charity.

### **3.2 Organisations’/Clients View about Electronic Banking**

With changing bank technology more and more organisations are likely to consider moving away from paper based banking methods; many organisations have already done so. Broadly speaking organisations will be justified in deciding to use electronic banking if:

- they can identify overall advantages for the organisation in doing so;
- they put in place adequate financial controls; and
- they have, or can acquire, the necessary legal power.

It is important that any decision to adopt electronic banking be made with the benefits and advantages to the organisation in mind. It is not right to move to electronic banking just because it seems fashionable or because the bank wants it to change (the motive for this might be to help the bank to reduce its own costs, rather than to provide a better service for the organisation).

With electronic banking we would expect the same level of internal financial controls as we would wish the traditional forms of banking. There should continue to be clear segregation of duties to prevent any single person from being able to control substantial resources or obtaining unauthorised access to information; and there should be proper approval at, or delegated from, trustee level for movements and payments from bank accounts

### 3.2.1 Electronic Banking Services

Electronic banking offers several services that consumers may find practical:

**Automated Teller Machines** or 24-hour tellers are electronic terminals that let your bank be on transaction almost any time. To withdraw cash, make deposits, or transfer funds between accounts, you generally insert an ATM card and enter your PIN. Some financial institutions and ATM owners charge a fee, particularly to consumers who don't have accounts with them or on transactions at remote locations. Generally, ATMs must tell you they charge a fee and its amount on or at the terminal screen before you complete the transaction. Check the rules of your institution and the ATMs you use to find out when or whether a fee is charged.

**Direct Deposit** lets you authorise specific deposits, such as paychecks and social security checks, to your account on a regular basis. You also may pre-authorise direct withdrawals so that recurring bills, such as insurance premiums, mortgages, and utility bills, are paid automatically. Be cautious before you pre-authorise direct withdrawals to pay sellers or companies with whom you are unfamiliar; funds from your bank account could be withdrawn fraudulently.

**Pay-by-Phone Systems** let you call your financial institution with instructions to pay certain bills or to transfer funds between accounts. You must have an agreement with the institution to make such transfers.

**Personal Computer Banking** lets you handle many banking transactions via your personal computer. For instance, you may use your computer to view your account balance, request transfers between accounts, and pay bills electronically.

**Debit Card Purchase Transactions** let you make purchases with a debit card, which also may be your ATM card. This could occur at a store or business, on the Internet or online, or by phone. The process is similar to using a credit card, with some important exceptions. While the process is fast and easy, a debit card purchase transfers money — fairly quickly — from your bank account to the company's account. So it is important that you have funds in your account to cover your purchase. This means you need to keep accurate records of the dates and amounts of your debit card purchases and ATM withdrawals in addition to any checks you write. Also be sure you know the store or business before you provide your debit card information, to avoid the possible loss of funds through fraud. Your liability for unauthorised use, and your rights for error resolution, may differ with a debit card.

**Electronic Cheque Conversion** converts a paper cheque into an electronic payment in a store or when a company receives your cheque in the mail. In a store, when you give your cheque to a cashier, the cheque is run through an electronic system that captures your banking information and the amount of the cheque. You're asked to sign a receipt and you get a copy for your records. When your cheque has been handed back to you, it should be voided or marked by the merchant so that it can't be used again. The merchant electronically sends information from the cheque (but not the cheque itself) to your bank or other financial institution, and the funds are transferred into the merchant's account. When you mail-in a cheque for payment to a merchant or other company, they may electronically send information from your cheque (but not the cheque itself) through the system, and the funds are transferred into their account. For a mailed cheque, you should still receive advance notice from a company that expects to send your cheque information through the system electronically. The merchant or other company might include the notice on your monthly statement or under its terms and conditions. The notice also should state if the merchant or company will electronically collect from your account a fee — like a "bounced cheque" fee — if you have insufficient funds to cover the transaction.

Be especially careful in Internet and telephone transactions that may involve use of your bank account information, rather than a cheque. A legitimate merchant that lets you use your bank account information to make a purchase or pay on an account should post information about the

process on their website or explain the process over the telephone. The merchant also should ask for your permission to electronically debit your bank account for the item you're purchasing or paying on. However, because Internet and telephone electronic debits don't occur face-to-face, you should be cautious with whom you reveal your bank account information. Don't give this information to sellers with whom you have no prior experience or with whom you have not initiated the call, or to companies that seem reluctant to provide information or discuss the process with you.

Not all electronic fund transfers are covered by the EFT Act. For example, some financial institutions and merchants issue cards with cash value stored electronically on the card itself. Examples include prepaid telephone cards, mass transit passes, and some gift cards. These "stored-value" cards, as well as transactions using them, may not be covered by the EFT Act. This means you may not be covered for the loss or misuse of the card. Ask your financial institution or merchant about any protections offered for these cards.

### **3.3 What Are the Advantages and Potential Difficulties of Electronic Banking?**

#### **Advantages**

- For organisations who give their own time it means that they can carry out banking out of working hours in the evenings and at weekends. Customers are able to carry out transactions 24 hours a day, 7 days a week and will no longer be restricted to bank opening hours.
- Customers can instantly see what is happening with their money rather than waiting for statements to be sent.
- There is no time spent queuing or journey time to travel to and from the bank for clients or employees of the organisation.
- Electronic banking enables individual branches to have their own local accounts but enables the organisations to access information regarding the bank balances of each branch. This may help the customers to exercise greater control over branch finances and may enable the funds of all the branches to be added together to secure a more favourable rate of interest.

#### **Potential Difficulties**

- Unless organisations and clients already own computer equipment there will be an initial financial outlay to establish computer banking.



This will involve the purchase and maintenance of a computer and the establishment of a telephone line.

- To use telephone banking there is the cost of the telephone calls to the bank, although these are usually charged at a local rate.
- For organisation or clients that have more than a basic computer banking service there may be a charge for the services of the bank.
- Computer banking requires some personal computer skills although banks and building societies are making efforts to make their software as “user friendly” as they can.
- An organisation or client may have used the same banking systems for many years and may find a new arrangement initially more complicated to understand and operate. It will also mean having to adapt and to modify existing internal financial controls.
- The need for an indemnity

### **3.4 Is Electronic Banking as Secure as More Traditional Methods of Banking?**

Security problems arise in a variety of ways: what is perceived as the key issue varies from place to place and from business to business. Worries about “the government knowing everything I do” are surprisingly common, particularly in areas with comparatively recent histories of robust internal security forces. Worries that “the tax authorities will know how large my turnover (or sometimes even personal expenditure) is” are particularly common in areas with a thriving black economy. Most pervasive, however, are the classic business worries about assurance of payment for the seller and assurance of delivery to specification for the buyer; as a sub-set of this, there are worries about the security of both banking and trading online against the depredations and disruptions of hackers.

Typical of views about security of trading is that expressed by Rupert Gavin, who is Director of Internet and Multimedia Services for British Telecom, expressed in February 1997.

“As the Internet matures and the number of users double monthly, businesses are keen to exploit the next natural phase - selling their goods and services to a vast audience. But trading over the World Wide Web has been hampered by a lack of trust in the security of online credit card transactions.”

In the same month, a computer hackers' club in Germany gave a public demonstration of unauthorised methods of transferring money from online bank accounts, leading to the following comment from Cornelius Villis of Microsoft, responsible for the Active X security model involved: “This is going to be the first of many incidents. Users are going to have to become very security conscious. We've been much too

sanguine.” A demonstration of potential fraud is very different from an achieved crime, of course, but such events both highlight the problem and also lead to fear and confusion among potential users. As a final example of the ways in which security problems can arise in quite unexpected ways, a case arose in California in 1993 in which an employee who had been dismissed, claimed that the dismissal was not for legitimate reasons but rather was the result of improper pressure applied by her alleged ex-lover, a director of the company. Her evidence was an e-mail which the court found to have been faked by her, and sent on the internal network of one of the world's largest and most successful software companies, which had (at the time) virtually no protection against fraudulent use.

Fortunately, these commonplace problems are very rapidly generating commonplace answers, sometimes in the form of commercial products or services (e.g. the Open Market Inc software for online credit card authorisation), and sometimes in the widespread use of techniques that are effectively in the public domain. (e.g. P.G.P. encryption)

In addition, electronic banking services are used increasingly by small and large organisations all over the world. Organisations and banks have a vested interest in making sure that electronic banking is as secure as possible.

Banks have a password system for both computer and telephone banking. With telephone banking all telephone calls are recorded, so cheques can be made if there are queries about a transaction. Care has to be taken by a charity to ensure that only trusted people have access to the passwords.

Systems can operate hierarchical passwords so that some people are given "read only" access (i.e. the ability to read information but not to change it or add to it), while others may be able to suggest changes which then need to be activated by a supervisor.

Some banks or building societies will offer arrangements where two or more people each have to enter their own password or personal number before transactions are effected. Some banks allow larger organisations to purchase a plastic card reader: when a payment or transfer has to be made each official can swipe their card (connected to their PC) and then enter a personal number to release the payment. In this way, one official cannot effect a transaction without other officials being made aware of it and being required to authorise it. Some banks have plans to bring in systems that involve electronic signatures or other advanced identification systems.

Whatever arrangements an organisation uses, the customers should prevent any one individual from being able to control significant resources.

### 3.5 People's Opinion

The majority of respondents to a recent Motorola survey said they would feel comfortable using Smartcard technology for the following:

- As a driving licence 73%
- As an ID card 70%
- As a passport 64%
- As an electronic purse 63%
- As a social security benefits card 61%

The market is therefore ready and waiting for electronic banking, whether that means using Internet web-based online banking, or alternatively (or additionally) Smartcard technology. Some services already exist:

- Bank of Scotland [www.bankofscotland.co.uk](http://www.bankofscotland.co.uk)
- Deutsche Bank [www.deutsche-bank.de](http://www.deutsche-bank.de)
- Estonian Savings Bank [www.esb.ee](http://www.esb.ee)
- Lloyds Bank and TSB [www.lloydstsb.co.uk](http://www.lloydstsb.co.uk)

Minitel banking in France is potentially available to 15 million users and is on course of migration to internet compatibility. T-Line videotext in Germany has approximately one million users for its on-line banking services.

However, Chip Maham, chief executive officer of Security First Network Bank (SFNB) of Atlanta ([www.sfnb.com](http://www.sfnb.com)) which operates entirely on the Internet, says the web is still too slow and clunky for some consumers. "The Web is not yet ready for prime time", he says. A survey of bankers by Grant Thornton consultants this year found that two-thirds were concerned about the security of online transactions. Half said their customers were, too.

Introducing online banking, however, does not mean that banks can eliminate all the other costly distribution channels they have built up over the years. In particular, they cannot close their branches - and shouldn't, if they want to keep their customers. "The future of e-commerce in retail banking is an AND process, not an OR process," says Tim Jones, Director of Retail Banking at National Westminster Bank ([www.natwest.co.uk/](http://www.natwest.co.uk/)) in the UK. Nat-West is currently trimming about 250 more branches out of its network, but has no plans to go below 1,750 branches for the foreseeable future. John Cleghorn,

Chairman and Chief Executive of the Royal Bank of Canada, would agree. "We have found rapid branch closures cost you market share, guaranteed. You can make a big mistake thinking everybody wants to deal with you on a PC," he says.

### 3.6 Other Concerns about Electronic Banking

**Databases:** There is concern that many valuable, factually-oriented databases may be denied copyright protection, or that courts may determine infringement in ways that severely limit the scope of copyright protection for databases. The unfair extraction right proposed in the EU database directive could protect such databases. Additionally, if multimedia works are regarded at international level as works in a new, separate category, the issue of their coverage under the existing conventions, and rules of national treatment will be open to debate. If, however, as current discussions seem to indicate, they are subsumed in the existing categories of works, establishing meaningful rules internationally will be simplified.

**Sound Recordings:** many believe that the time has come to bring protection for the performers and producers of sound recordings into line with the protection afforded to the creators of other works, since there is no just reason to accord a lower level of protection to one special class of creative artists, and since the digital communications revolution - the creation of advanced information infrastructures - is erasing the distinctions among different categories of protected works and sound recordings and the uses made of them. There is also a specific issue about the extent and scope of moral rights in the world of digital communications. Some believe that the ability to modify and restructure existing works and to create new multimedia works make moral rights more important than ever before. Others take the view that careful thought must be given to the scope, extent, practicality and especially the waive-ability of moral rights in respect of digitally fixed works, sound recordings and other information products.

**Rights Clearance Services:** For many years, intellectual property rights holders have benefited from organisations collecting the numerous small sums that accrue from, for instance, public performance of recorded music. Electronic commerce not only extends the issues (as above) but also helps provide solutions.

### 3.7 Benefits of Online Banking: Case Study of Washington Mutual Bank

- (1) **It's FREE.** We don't charge for online banking or to pay bills online from a WaMu checking account.

- (2) **It's FAST.** There's no complicated software to download or learn. Just register and set up your user name and password, and you're ready to go!
- (3) **It's SECURE.** You can bank online at wamu.com with confidence. Our security features are designed to guard your personal information. In the unlikely event that a fraudulent online banking transaction occurs while on our site, our [online banking](#) guaranteed means that you won't be liable.
- (4) **To sign up,** it just takes a couple of minutes. [Sign up now.](#)
- (5) **Not sure if online banking is for you?** Check out our interactive demo of Online Banking features.

### 3.7.1 More Reasons to Sign up for Online Banking

Get account information at your convenience. Why wait for paper statements to balance your checkbook? With Personal Online Banking, you can:

- (1) **See account details** for your eligible checking, savings, CD, loan, line of credit and mortgage accounts.
- (2) **Check account balances** and payment history.
- (3) **Transfer funds** between eligible Washington Mutual deposit accounts—and schedule future transfers.
- (4) **Download account information** to Personal Financial Management software, such as Quicken or Microsoft Money.
- (5) **Save shredding time (and trees)**—if you sign up to receive Online Statements, you can opt to stop getting paper statements in the mail.
- (6) **Stay informed** with Account Alerts. Choose the type of alerts you want, and you'll receive e-mail whenever your account changes.

Pay bills online – free of fees. Kick the check-writing habit—and kiss envelopes, stamps and stacks of paper goodbye. With our online Personal Bill Pay® service, you can:

- (a) **Pay virtually anyone in the United States** from your eligible checking account.
- (b) **Schedule payments** in advance—both one-time and recurring payments.
- (c) **Pay multiple bills** quickly, from the same screen.
- (d) **18 months of your bill payment history.**
- (e) **Get a great deal**—no matter how many bills you pay each month, Personal Bill Pay service is free (subject to funds availability, of course).

Pay bills on time – guaranteed. You won't have to worry about bill payments being late with our Personal Bill Pay service. When you initiate your payment four business days before the due date, you get our **On Time Guarantee**. To take part, just remember to:

- (a) Schedule the first payment to each payee four (4) business days before the due date.
- (b) Schedule the next payments two (2) business days before the due date for a payment that is made electronically and four (4) business days before the due date for a payment made by check.
- (c) You will know whether the On Time Guarantee is two (2) business days or four (4) business days before the due date by the Estimated Due Date (Deliver By Date) shown at the time you schedule your payment. (Due date does not include grace period, if any).
- (d) Provide accurate payment instructions.
- (e) Make sure you have available funds in your account to cover the payment.
- (f) Not make a "restricted" payment, such as a court-ordered tax, securities settlement or international payment.

Servicing your accounts: No more mail, phone calls or trips to the bank to service your accounts. Instead, you can just log on to:

- (a) **Order new checks**—even order different styles for your checking account!
- (b) **Stop a payment** on a deposit account check.
- (c) **Order copies of checks** or paper statements.
- (d) **Update your address**.

#### 4.0 CONCLUSION

E-banking offers potentials to facilitate and bring about efficiency and convenience in the banking industry. These potentials are being explored despite the obvious difficulties arising from security threats and fraud. E-banking is undergoing a process and will get better by the day. However, it seems practically impossible to eliminate the potential security threats and fraud, but they can be minimised.

#### 5.0 SUMMARY

After the invention of paper, most of the organisations including government organisations and banks march on paper. Nevertheless, as

information technology evolves the new technology has to play a part in helping the process of organisations.

- For many consumers, electronic banking means 24-hour access to cash through an Automated Teller Machine (ATM) or Direct Deposit of paychecks into checking or savings accounts.
- With changing bank technology more and more organisations are likely to consider moving away from paper based banking methods; many organisations have already done so
- Electronic banking offers several services that consumers may find practical.
- Debit Card Purchase Transactions let you make purchases with a debit card, which also may be your ATM card. This could occur at a store or business, on the Internet or online, or by phone.
- Be especially careful in Internet and telephone transactions that may involve use of your bank account information, rather than a cheque. A legitimate merchant that lets you use your bank account information to make a purchase or pay on an account should post information about the process on their website or explain the process over the telephone
- Not all electronic fund transfers are covered by the EFT Act. For example, some financial institutions and merchants issue cards with cash value stored electronically on the card itself
- Security problems arise in a variety of ways : what is perceived as the key issue varies from place to place and from business to business. Worries about "the government knowing everything I do" are surprisingly common, particularly in areas with comparatively recent histories of robust internal security forces
- Minitel banking in France is potentially available to 15 million users and is on course of migration to Internet compatibility. T-Line videotext in Germany has approximately 1 million users for its online banking services.
- There is concern that many valuable, factually-oriented databases may be denied copyright protection, or that courts may determine infringement in ways that severely limit the scope of copyright protection for databases
- For many years, intellectual property rights holders have benefited from organisations collecting the numerous small sums that accrue from, for instance, public performance of recorded music.
- Why wait for paper statements to balance your chequebook? With Personal Online Banking, you can.

## **6.0 TUTOR– MARKED ASSIGNMENT**

1. Mention five services operating electronic banking.

2. Briefly discuss five potential difficulties for the client, in operating electronic banking

## **7.0 REFERENCES/FURTHER READINGS**

Beep Good Practice Knowledge Base (2006). *Electronic Banking*.

Charity Organisation Report (2005). *Guidance on Electronic Banking*.

Chaudhury, Abijit, Jean-Pierre Kuilboer (2002). *e-Business and e-Commerce Infrastructure*. McGraw-Hill.

## **UNIT 2 INTRODUCTION TO E-BANKING (2): TYPES OF ELECTRONIC BANKING**

### **CONTENTS**

- 1.0 Introduction



2.0	Objectives
3.0	Main Content
3.1	The Virtual Bank
3.2	History
3.3	Mobile Banking
3.3.1	Trends in Mobile Banking
3.3.2	Mobile Banking Services
3.3.3	Challenges for Mobile Banking Solution
3.4	Telephone Banking
3.5	Electronic Fund Transfer
3.5.1	Card-Based EFT
3.5.2	Debit Card EFT
3.6	Wire Transfer
3.6.1	History
3.6.2	Overview of Process
3.6.3	Regulation
3.6.4	Security Features
3.6.5	Methods of Transfer
3.7	Automated Clearing House
3.7.1	Uses of the ACH Payment System
3.7.2	ACH Process
3.7.3	Some Issues with ACH
3.8	Internet Banking
4.0	Conclusion
5.0	Summary
6.0	Tutor-Marked Assignment
7.0	References/Further Readings

## **1.0 INTRODUCTION**

For many consumers, electronic banking means 24-hour access to cash through an Automated Teller Machine (ATM) or Direct Deposit of paychecks into checking or savings accounts. But electronic banking now involves many different types. These types differ based on services offered and the extent of those services. In most cases they offer the same type of services.

## **2.0 OBJECTIVES**

At the end of this unit, you should be able to:

- list the different forms of e-banking
- enumerate the services offered by the forms of e-banking

- state the trend guiding some of the forms of e-banking
- answer the question of the challenges facing the forms of e-banking.

### 3.0 MAIN CONTENT

#### 3.1 The Virtual Bank

A **virtual bank** is a bank with a very small or nonexistent branch network. It offers its financial services by:

- Telephone Banking
- Online Banking
- Automated Teller Machine
- Mail Banking
- Mobile Banking

By eliminating the costs associated with retail banking, particularly bank branches, virtual banks may offer higher interest rates and lower service charges on their savings accounts than their competitors.

#### 3.2 History

Traditional banking was impacted greatly by the commercialisation of the Internet in the early 1990s. As the Internet became more generally accessible, traditional banks began to realise its potential to deliver services to their customers while reducing long-term operational costs. Upon realising this, traditional banks began to offer limited services online.

The initial success of Internet banking services provided by traditional banks led to the development of Internet-only banks or "virtual banks". These banks were designed without a traditional banking infrastructure, a cost-saving feature that allowed many of them to offer savings accounts with higher interest rates and loans with lower interest rates than most traditional banks.

The initial success of Internet banking services provided by traditional banks led to the development of Internet-only banks or "virtual banks". These banks were designed without a traditional banking infrastructure, a cost-saving feature that allowed many of them to offer savings accounts with higher interest rates and loans with lower interest rates than most traditional banks.

The world's first fully-functional virtual bank was the Security First Network Bank (SFNB) which began operations on October 18, 1995. Based at Atlanta Georgia, USA, it was the first virtual bank to be

insured by the Federal Deposit Insurance Corporation (FDIC). After three years of operation, it was acquired by the Royal Bank of Canada (RBC). Though SFNB did not make much profit in the initial years, it demonstrated that the concept of virtual banking could work.

Europe's first full-service virtual bank was "First-e" launched by Enba, a Dublin-based company under the banking license of *Banque d'Escompte*, France. First launched in the UK in late September 1999, it garnered appreciable attention, resulting in more such ventures all over Europe. After about two years of operations, it shut down its operations during the dot-com bubble bust. Though Egg Bank, launched earlier in October 1998 by Prudential Plc was touted to be a virtual bank, it was not a full-service virtual bank initially.

Asia's first virtual bank was finatiQ— a division of the Bank of Singapore. It opened on April 3, 2000 (though the public launch was on April 18, 2000), heralding the arrival of virtual banking in Asia.

### 3.3 Mobile Banking

**Mobile Banking** (also known as M-Banking or mBanking) is a term used for performing transactions, payments etc. via a mobile device such as a mobile phone. Mobile banking is normally accessed via SMS or the mobile Internet.

- Mobile banking consists of three inter-related applications:
- Mobile accounting
- Mobile brokerage
- Mobile financial information services

Most services in accounting and brokerage are transaction based. The non-transaction based services of informational nature are however imperative for conducting transactions. For instance, balance inquiries might be needed before committing a money remittance. The accounting and brokerage services are therefore offered invariably in combination with information services. Information services, on the other hand, may be offered as an independent module.

#### 3.3.1 Trends in Mobile Banking

The advancement of the Internet has revolutionised the way the financial services industry conducts business. It has empowered organisations with new business models and new ways to offer (24 x 7) accessibility to their customers. The ability to offer financial transactions online has created new players in the financial services industry, such as online banks, online brokers and wealth managers who offer personalised

services. Over the last few years, the mobile and wireless market has been one of the fastest growing and most interesting markets in the world. It is still growing at a rapid pace. A recent study done by In-Stat/MDR, claims that the number of mobile subscribers worldwide will reach 2 billion before the end of 2007. Mobile users have just started to fully utilise the data capabilities in their mobile phones. In Asian countries like India, China, Indonesia and Philippines, where mobile infrastructure is comparatively better than the fixed-line infrastructure and in European countries where mobile phone penetration is very high (80% of consumers use a mobile phone), mobile phone banking is likely to appeal even more.

This opens up a huge market for financial institutions interested in offering value added services. With mobile technology, banks can offer a wide range of services to their customers such as doing funds transfer while traveling, receiving online updates of stock price or even performing stock trading while being stuck in traffic. According to the German mobile operator Mobilcom, mobile banking will be the killer application for the next generation of mobile technology.

Mobile devices, especially smartphones, are the most promising way to reach the masses and to create “stickiness” among current customers, due to their ability to provide services anytime, anywhere, high rate of penetration and potential to grow. According to Gartner, shipment of smartphones is growing fast, and should top 20 million units in 2006 alone.

In the recent past, banks across the globe have invested billions of dollars to build sophisticated internet banking capabilities. As the trend is shifting to mobile banking, there is a challenge for CIOs and CTOs of these banks to decide on how to leverage their investment in internet banking and offer mobile banking, in the shortest possible time.

The proliferation of the 3G (third generation of wireless) and widespread implementation expected for 2003-2007 will generate the development of more sophisticated services such as multimedia and links to m-commerce services.

### **3.3.2 Mobile Banking Services**

#### **Accounting Information**

1. Mini-statements and checking account
2. Term deposit
3. Loans statement
4. Cards statement

5. Mutual funds / Equity statement
6. Insurance policy
7. Pension plan

### **Payments and Transfer**

1. Domestic and international fund transfers
2. Micro-payments
3. Mobile re-charge
4. Commercial payments
5. Bill payment

### **Investments**

1. Portfolio Management Services
2. Real-time stock quotes
3. Personalised alerts and notifications on security prices

### **Support**

1. Status of origination of mortgage, insurance
2. Check book request
3. Exchange data message and email / complaints

### **Content Services**

1. General information such as weather updates, news
2. Loyalty related offers
3. Location dependent services

Based on survey conducted by Forrester, mobile banking will be attractive mainly to the younger, more tech-savvy customer segment. A third of mobile phone users say that they may consider performing some kind of financial transaction through their mobile phone. But most of the users are interested in performing basic transactions such as querying for account balance and making bill payment.

### **3.3.3 Challenges for a Mobile Banking Solution**

The challenges in developing a sophisticated mobile banking application are:

- **Interoperability:** There is a lack of common technology standards for mobile banking. Many protocols are being used for mobile banking – HTML, WAP, SOAP, XML to name a few. It would be a

wise idea for the vendor to develop a mobile banking application that can connect multiple banks. It would require either the application to support multiple protocols or use of a common and widely acceptable set of protocols for data exchange. There are a large number of different mobile phone devices and it is a big challenge for banks to offer mobile banking solution on any type of device. Some of these devices support J2ME and others support WAP browser or only SMS.

- **Security:** Security of financial transaction, being executed from some remote location and transmission of financial information over the air, are the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the bank's IT department.

The following aspects need to be addressed to offer a secure infrastructure for financial transaction over wireless network:

- Physical security of the hand-held device. If the bank is offering smart-card based security, the physical security of the device is more important.
- Security of the thick-client application running on the device. In case the device is stolen, the hacker should require ID/Password to access the application.
- Authentication of the device with service provider before initiating a transaction. This would ensure that unauthorised devices are not connected to perform financial transactions
- User ID / password authentication of bank's customer
- Encryption of the data being transmitted over the air.
- Encryption of the data that will be stored in device for later / off-line analysis by the customer
- **Scalability and Reliability:** Another challenge for the CIOs and CTOs of the banks is to scale-up the mobile banking infrastructure to handle exponential growth of the customer base. With mobile banking, the customer may be sitting in any part of the world (a true anytime, anywhere banking) and hence banks need to ensure that the systems are up and running in a true 24 x 7 fashion. As customers will find mobile banking more and more useful, their expectations from the solution will increase. Banks unable to meet the performance and reliability expectations may lose customer confidence.
- **Application distribution:** Due to the nature of the connectivity between a bank and its customers, it would be impractical to expect customers to regularly visit banks or connect to a web site for regular

upgrade of their mobile banking application. It will be expected that the mobile application itself check the upgrades and updates and download necessary patches. However, there could be many issues to implement this approach such as upgrade / synchronisation of other dependent component.

- **Personalisation:** It would be expected from the mobile application to support personalisation such as:
  - i. Preferred Language
  - ii. Amount format
  - iii. Date / Time format
  - iv. Default transactions
  - v. Standard Beneficiary list
  - vi. Alerts

### 3.4 Telephone Banking

**Telephone banking** is a service provided by a financial institution which allows its customers to perform transactions over the telephone. Most telephone banking operators use an automated phone answering system with phone keypad response or voice recognition capability. To guarantee security, the customer must first authenticate through a numeric or verbal password or through security questions asked by a live representative (see below). With the obvious exception of cash withdrawals and deposits, it offers virtually all the features of an automated teller machine: account balance information and list of latest transactions, electronic bill payments, fund transfers between a customer's accounts, etc. Usually, there is also the possibility to speak to a live representative located in a call centre or a branch, although this feature is not guaranteed to be offered 24/7. In addition to the self-service transactions listed earlier, telephone banking representatives are usually trained to do what was traditionally available only at the branch: loan applications, investment purchases and redemptions, chequebook orders, debit card replacements, change of address, etc.

Banks which operate mostly or exclusively by telephone are known as phone banks.

### 3.5 Electronic Fund Transfer

**Electronic Funds Transfer** or **EFT** refers to the computer-based systems used to perform financial transactions electronically.

The term is used for a number of different concepts:

- cardholder-initiated transactions, where a cardholder makes use of a payment card
- electronic payments by businesses, including salary payments
- electronic check (or cheque) clearing.

### 3.5.1 Card-Based EFT

**Credit Card.** EFT may be initiated by a cardholder when a payment card such as a credit card or debit card is used. This may take place at an Automated Teller Machine (ATM) or Point of Sale (EFTPOS), or when the card is not present, which covers cards used for mail order, telephone order and Internet purchases.

Card-based EFT transactions are often covered by the ISO 8583 standard.

#### Transaction Types

A number of transaction types may be performed, including the following:

- **Sale:** where the cardholder pays for goods or service
- **Refund:** where a merchant refunds an earlier payment made by a cardholder
- **Withdrawal:** the cardholder withdraws funds from their account, e.g. from an ATM. The term *Cash Advance* may also be used, typically when the funds are advanced by a merchant rather than at an ATM
- **Deposit:** where a cardholder deposits funds to their own account (typically at an ATM).
- **Cashback:** where a cardholder withdraws funds from their own account at the same time as making a purchase.
- **Inter-Account Transfer:** transferring funds between linked accounts belonging to the same cardholder
- **Payment:** transferring funds to a third party account
- **Inquiry:** a transaction without financial impact, for instance balance inquiry, available funds inquiry, linked accounts inquiry, or request for a statement of recent transactions on the account
- **Administrative:** this covers a variety of non-financial transactions including PIN change

The transaction types offered depend on the terminal. An ATM would offer different transactions from a POS terminal, for instance.

#### Authorisation



EFT transactions require communication between parties. When a card is used at a merchant or ATM, the transaction is first routed to an [acquirer](#), then through a number of networks to the issuer where the cardholder's account is held.

A transaction may be authorised *offline* by any of these entities through a stand-in agreement. Stand-in authorisation may be used when a communication link is not available, or simply to save communication cost or time. Stand-in is subject to the transaction amount being below agreed limits. These limits are calculated based on the risk of authorising a transaction offline, and thus vary between merchants and card types. Offline transactions may be subject to other security checks such as checking the card number against a 'hotcard' (stolen card) list, velocity checks (limiting the number of offline transactions allowed by a cardholder) and random online organisation.

A transaction may be authorised via a *pre-authorization* step, where the merchant requests the issuer to reserve an amount on the cardholder's account for a specific time, followed by *completion*, where the merchant requests an amount blocked earlier with a pre-authorisation. This transaction flow in two steps is often used in businesses such as hotels and car rental where the final amount is not known, and the pre-authorisation is made based on an estimated amount. Completion may form part of a *settlement* process, typically performed at the end of the day when the day's completed transactions are submitted.

## Authentication

EFT transactions may be accompanied by methods to authenticate the card and the cardholder. The merchant may manually verify the cardholder's signature, or the cardholder's personal identification number (PIN) may be sent online in an encrypted form for validation by the card issuer. Other information may be included in the transaction, some of which is not visible to the cardholder (for instance magnetic stripe data), and some of which may be requested from the cardholder (for instance the cardholder's address or the CVV2 value printed on the card).

EMV cards are smartcard-based payment cards, where the smartcard technology allows for a number of enhanced authentication measures.

### 3.5.2 Debit Card EFT

A **debit card** is a plastic card which provides an alternative payment method to cash when making purchases. Physically the card is an ISO 7810 card like a credit card; however, its functionality is more similar to

writing a cheque as the funds are withdrawn directly from either the cardholder's bank account (often referred to as a *cheque card*), or from the remaining balance on a gift card.

Depending on the store or merchant, the customer may swipe or insert their card into the terminal, or they may hand it to the merchant who will do so. The transaction is authorised and processed and the customer verifies the transaction either by entering a PIN or, occasionally, by signing a sales receipt.

In some countries the debit card is multipurpose, acting as the automated teller machine card for withdrawing cash and as a cheque guarantee card. Merchants can also offer "cashback"/"cashout" facilities to customers, where a customer can withdraw cash along with their purchase.

The use of debit cards has become wide-spread in many countries and has overtaken the cheque and in some instances cash transactions by volume. Like credit cards, debit cards are used widely for telephone and Internet purchases. This may cause inconvenient delays at peak shopping times (e.g. the last shopping day before Christmas), caused when the volume of transactions overloads the bank networks.

### 3.6 Wire Transfer

A **wire transfer** is a method of transferring of funds from one entity to another. Wire transfers can be done by a simple bank account transfer, or by a transfer of cash at a cash office.

#### 3.6.1 History

Although the genesis of the idea dates as far back as the [giro](#), the modern wire transfer was a product of the telegraph companies, which made it possible to wire a money order from one office to another. Later, it became possible to wire money between banks, which is essentially the same process as the giro.

In modern times, the word *wire transfer* or *bank transfer* (sometimes combined as *bank wire transfer*) is used for domestic or international transactions where no cash or cheque exchange is involved, but the account balance is directly (electronically) transferred from one bank to the other. A transfer might be done to support relatives, rescue travelers in unexpected emergencies, or to pay a business transaction.

#### 3.6.2 Overview of Process

Bank wire transfers are often the most expedient method for transferring funds between bank accounts. A bank wire transfer is affected as follows:

- i. The sending bank transmits a secure message (via a secure system such as SWIFT, or Fedwire) to the receiving bank, requesting that they effect payment in accordance with the instructions
- ii. The message also includes settlement instructions. The actual wire transfer itself is virtually instantaneous, requiring no longer for transmission than a telephone call.
- iii. The banks involved must either hold a reciprocal account with each other, or the payment must be sent to a bank with such an account, or a correspondent bank, for further benefit to the ultimate recipient.

### **3.6.3 Regulation**

Bank transfer is the most common payment method in Europe with several million transactions done each day. While in 2002 the European Commission has regulated the fees banks may charge for payments in Euro between European Union member countries down to the domestic level (see the Regulation (EC) No 2560/2001 of the European Parliament and of the Council of 19 December 2001), resulting in either very low or no fees for transfers within the eurozone, international wire transfers outside this limited scope can be quite expensive.

In the United States, wire transfers within the country are governed by the following regulations:

- Federal Regulation J
- Article 4A of the Uniform Commercial Code

### **3.6.4 Security Features**

Wire transfer, done bank-to-bank, is considered the safest international payment method. Both account holders must have a proven identity, and there is little possibility of a chargeback, although wires can be recalled. Additionally, information contained in wires is transmitted securely through encrypted communications methods. The price of bank wire transfers vary widely depending on the bank and its location and in some countries the fee associated with the service can be costly.

Wire transfers done through cash offices, however, are more-or-less anonymous and designed for funds transfer between persons who trust each other. It is unsafe to send money by wire for an unknown person to be collected at a cash office. The receiver of the funds may, after collecting them, simply disappear. This method of scam has been often used especially in so-called and also known as advance fee fraud or a “419” scam.

Transfers in the United States are subject to monitoring by the Office of Foreign Assets Control, or OFAC. OFAC monitors information provided in the text of the wire to determine if money is being transferred to terrorist organisations or countries or entities currently under sanction by the United States government. If a financial institution suspects that funds are being sent from or to one of these entities, they must block the transfer and freeze the funds.

### **3.6.5 Methods of Transfer**

#### **1. Western Union**

One of the largest companies that offer wire transfer is Western Union (minimum of £25 in the UK, or \$15 in the US). Western Union began in 1851 in Rochester, New York, and became the preeminent telegraph transfer service. It also introduced Telex, which was a predecessor of today's wire transfer services and is still used by some banks and business entities. Initially based in the United States, the company expanded operations internationally in 1989.

Western Union is a stand-alone entity and is not affiliated with a financial institution. Individuals who transfer or receive money with Western Union do not need to have an account with Western Union, or any financial institution. Instead, transfer instructions are sent into a central system, and the recipient can pick up the funds at a Western Union office in their area. Western Union transfers can also be initiated online.

Concern and controversy about Western Union transfers have increased in recent years, due to the increased monitoring of money laundering transactions, as well as concern about terrorist groups using the service, particularly in the wake of 9/11. Although Western Union keeps information about senders and receivers, some transactions can essentially be done anonymously (ie, the receiver is not always obligated to show identification.).

#### **2. Country-to-Country Wire Transfer**

Most international, country-to-country transfers are executed using the SWIFT system. The co-operative society, Society for Worldwide Interbank Financial Telecommunication, or SWIFT, was founded in 1974 by seven international banks. SWIFT operates a world wide network to facilitate the transfer of financial messages. Using these messages, banks can exchange data for transfer of funds between different financial institutions. The Society's headquarters are situated in La Hulpe, on the outskirts of Brussels. S.W.I.F.T. also acts as a United Nations sanctioned International Standards body (ISO) for the creation and maintenance of financial messaging standards.

Article 3 of S.W.I.F.T. states that:

*“The object of the Company is for the collective benefit of the Members of the Company, the study, creation, utilisation and operation of the means necessary for the telecommunication, transmission and routing of private, confidential and proprietary financial messages”*

Each financial institution is provided an ISO 9362 code, also known as a Bank Identifier Code, BIC Code, or SWIFT Code. These codes are generally eight characters in length. As an example, Deutsche Bank is an international bank; its head office is based in Frankfurt, Germany. Its SWIFT code for its primary office is DEUTDEFF.

- DEUT identifies Deutsche Bank
- DE is the country code for Germany
- FF is the code for Frankfurt

Using an extended code of 11 digits (if the receiving bank has assigned branches or processing areas individual extended codes) allows the payment to be directed to a specific office. For example, DEUTDEFF500 would direct the payment to an office of Deutsche Bank in Bad Homburg.

European banks making transfers within the European Union also utilise the International Bank Account Number, or IBAN.

### 3.7 Automated Clearing House

**Automated Clearing House (ACH)** is the name of an electronic network for financial transactions in the United States. ACH processes large volumes of both credit and debit transactions which are originated in batches. Rules and regulations governing the ACH network are established by NACHA-The Electronic Payments Association, formerly the **National Automated Clearing House Association**, and the Federal

Reserve (Fed). In 2002, this network processed an estimated 8.05 billion ACH transactions with a total value of \$21.7 trillion. In the rest of the developed world, these rules and regulations are defined by each country's regulatory bodies. European Payments Council is currently implementing a PE-ACH, Pan-European ACH.

ACH credit transfers include direct-deposit payroll payments and payments to contractors and vendors. ACH debit transfers include consumer payments on insurance premiums, mortgage loans, and other kinds of bills. Businesses are also increasingly using ACH to collect from customer online, rather than accepting credit or debit cards.

Debit transfers also include new applications such as the Point-of-Purchase (POP) check conversion pilot program sponsored by NACHA. FedACH is the Federal Reserve's centralised application software used to process ACH transactions. Both the government and the commercial sectors use ACH payments. The Electronic Payments Network (EPN) is the only private sector ACH Operator in the United States.

The Federal Reserve Banks are collectively the nation's largest automated clearinghouse operator and in 2005 processed 60% of commercial interbank ACH transactions. The EPN processed the remaining 40%. EPN and the Reserve Banks rely on each other for the processing of some transactions in which either the Originating Depository Financial Institution (ODFI) or Receiving Depository Financial Institution (RDFI) is not their customer. These interoperator transactions are settled by the Reserve Banks.

### **3.7.1 Uses of the ACH Payment System**

- Direct deposit of payroll, social security and other government benefits, and tax refunds
- Direct payment of consumer bills such as mortgages, loans, utility bills, and insurance premiums
- Business-to-business (B2B) payments
- E-check
- E-commerce payments
- Federal, state, and local tax payments

### **3.7.2 ACH Process**

It is important to note that, in accordance with the rules and regulations of ACH, no financial institution may simply issue an ACH transaction (whether it be debit or credit) towards an account without prior authorisation from the account holder (known as the *Receiver* in ACH terminology).

An ACH entry starts with a *Receiver* authorising an *Originator* to issue ACH debit or credit to an account. An *Originator* can be a person or a company (such as the gas company, a local cable company, or one's employer). Depending on the ACH transaction, the *Originator* must receive written (ARC, POP, PPD), verbal (TEL), or electronic (WEB) authorisation from the *Receiver*. Written authorisation constitutes a signed form giving consent on the amount, date, or even frequency of the transaction. Verbal authorisation needs to be either audio recorded or the "Originator" must send a receipt of the transaction details before or on the date of the transaction. A WEB authorisation must include a customer reading the terms of the agreement and typing or selecting some form of an "I agree" statement.

Once authorisation is acquired, the *Originator* then creates an ACH entry to be given to an *Originating Depository Financial Institution* (ODFI), which can be any financial institution that does ACH origination. This ACH entry is then sent to an *ACH Operator* (usually the Fed) and is passed on to the *Receiving Depository Financial Institution* (RDFI), where the *Receiver's* account is issued either a credit or debit, depending on the ACH transaction.

The RDFI may, however, reject the ACH transaction and return it to the ODFI with the appropriate reason, such as that there were insufficient funds in the account or that the account holder indicated that the transaction was unauthorised. An RDFI has a prescribed amount of time in which to perform returns, ranging from 2 to 60 days from the receipt of the ACH transaction. However, the majority of transactions, if going to be returned are done so within 24 hours from midnight of the day the RDFI receives the transaction.

An ODFI receiving a return of an ACH entry may re-present the ACH entry two more times, or up to three total times, for settlement. Again, the RDFI may reject the transaction, after which the ODFI may no longer represent the transaction via ACH.

### **3.7.3 Some Issues with ACH**

ACH payments have been around for some time now, but people are just getting used to them, especially with the ARC, POP, and RCK, where the original instrument was a physical check. One issue occurs when the account holder issues a stop payment on a physical check not knowing that the check was presented as an ACH entry.

A timeframe issue can cause potential loss towards an RDFI due to irregular timeframes provided for the return of ACH entries that are subject to Regulation E. An example is a POP and ARC entry, where an

RDFI has only 60 days from the date of settlement to return an unauthorised debit, and the consumer has 60 days upon notification to dispute a transaction in his statement under Regulation E. With these timeframes, it is possible that the 60-day period allowed for ACH return would expire even before the consumer's 60-day protection (under Regulation E) would expire.

Another issue deals with compliance where the merchant causes an ODFI to issue an ARC or POP entry (for check presentment) and then fails to comply with the handling of the physical check and presents the physical check for payment as well. This causes a double-debit against a consumer account.

### 3.8 Internet Banking

This form of e-banking will be discussed as a separate unit. This is in view of its popularity and significance in the emerging electronic banking industry.

## 4.0 CONCLUSION

Different forms of e-banking will continually emerge as long as their corresponding emergence of information and communication technologies can be adopted for electronic banking. The relevance of these forms of e-banking is to offer the customers a wide variety of products and services which in turn makes banking operations more attractive and convenient.

## 5.0 SUMMARY

- For many consumers, electronic banking means 24-hour access to cash through an automated teller machine (ATM) or Direct Deposit of paychecks into checking or savings accounts.
- A **virtual bank** is a bank with a very small or non-existent branch network.
- Traditional banking was impacted greatly by the commercialisation of the [Internet](#) in the early 1990s. As the Internet became more generally accessible, traditional banks began to realise its potential to deliver services to their customers while reducing long-term operational costs
- Mobile Banking (also known as M-Banking or mBanking) is a term used for performing transactions, payments etc. via a mobile device such as a mobile phone.
- The advancement of the Internet has revolutionised the way the financial services industry conducts business. It has empowered



organisations with new business models and new ways to offer 24x7 accessibility to their customers

- Telephone banking is a service provided by a financial institution which allows its customers to perform transactions over the telephone. Most telephone banking use an automated phone answering system with phone keypad response or voice recognition capability
- Electronic Funds Transfer or **EFT** refers to the computer-based systems used to perform Financial Transactions electronically.
- EFT may be initiated by a cardholder when a payment card such as a credit card or debit card is used. This may take place at an automated teller machine (ATM) or point of sale (EFTPOS), or when the card is not present, which covers cards used for mail order, telephone order and internet purchases.
- A debit card is a plastic card which provides an alternative payment method to cash when making purchases.
- Bank wire transfers are often the most expedient method for transferring funds between bank accounts.
- Bank transfer is the most common payment method in Europe with several million transactions done each day.
- Most international, country-to-country transfers are executed using the SWIFT system. The co-operative society Society for Worldwide Interbank Financial Telecommunication, or SWIFT, was founded in 1974 by seven international banks.
- Automated Clearing House (ACH) is the name of an electronic network for financial transactions in the United States. ACH processes large volumes of both credit and debit transactions which are originated in batches.
- It is important to note that, in accordance with the rules and regulations of ACH, no financial institution may simply issue an ACH transaction (whether it be debit or credit) towards an account without prior authorisation from the account holder
- ACH payments have been around for some time now, but people are just getting used to them, especially with the ARC, POP, and RCK, where the original instrument was a physical check

## **6.0 TUTOR-MARKED ASSIGNMENT**

1. Mention five components of the **Accounting Information** service of a mobile bank
2. Discuss very briefly, five types of transactions in Card-based EFT

## **7.0 REFERENCES/FURTHER READINGS**

Buse, Stephan & Tiwari, Rajnish (2006). "The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking

Sector”. Research Project Mobile Commerce, University of Hamburg.

Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2006). *Customer on the Move: Strategic Implications of Mobile Banking for Banks and Financial Enterprises*, in: CEC/EEE 2006, Proceedings of The 8th IEEE International Conference on E-Commerce Technology and The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), San Francisco, pp. 522-529.

Tiwari, Rajnish; Buse, Stephan & Herstatt, Cornelius (2006). “Mobile Banking as Business Strategy: Impact of Mobile Technologies on Customer Behaviour and its Implications for Banks”, in: *Technology Management for the Global Future* - Proceedings of PICMET 06.

Owens, John & Anna Bantug-Herrera (2006). *Catching the Technology Wave: Mobile Phone Banking and Text-A-Payment in the Philippines*.

### **UNIT 3      INFORMATION SYSTEMS AUDITING FOR INTERNET BANKING**

#### **CONTENTS**

- 1.0    Introduction
- 2.0    Objectives
- 3.0    Main Content
  - 3.1    Internet Banking Activities
  - 3.2    Review of Internet Banking
    - 3.2.1    Scope

- 3.3 Independence
  - 3.3.1 Professional Objectivity
- 3.4 Competence
  - 3.4.1 Skills and Knowledge
- 3.5 Planning
  - 3.5.1 High-Level Risk Assessment
  - 3.5.2 Scope and Objectivity of the Review
  - 3.5.3 Approach
  - 3.5.4 Sign-Off for the Plan
- 3.6 Performance of Internet Banking Review
  - 3.6.1 Execution
  - 3.6.2 Aspects to Review
- 3.7 Reporting
  - 3.7.1 Report Content
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

## 1.0 INTRODUCTION

The term “Internet banking” refers to the use of the Internet as a remote delivery channel for banking services. Services include the traditional ones, such as opening an account or transferring funds to different accounts, and new banking services, such as electronic online payments (allowing customers to receive and pay bills on a bank’s website).

In March 1997, *Wired* magazine reported that more than half of the European banks recently surveyed by management consultants at Booz-Allen and Hamilton said that they would offer banking services over the Internet within a year, and more three-quarters said they would do so within three years.

Internet banking makes good sense for financial institutions. For about £1 million, less than the cost of building a single traditional branch, a bank can set up a fully functioning operation on the Internet. Booz-Allen were reported to have estimated that the cost of depositing a cheque with a real-live bank clerk over a branch counter is around 65 pence. By post and telephone, the cost of the same transaction is reduced. With a dial-up PC banking service, it halves again, to about 15p. With an Internet banking system, the cost drops below 5p, and sometimes as low as 1p.

This is particularly significant because electronic commerce opportunities for small and medium sized enterprises require a reliable and low cost electronic payment system. However, many electronic payment issues are institutional rather than technical. Creating the legal

framework for a world-wide electronic payment system will require substantial co-ordination and high level priority on the agenda of monetary authorities. This framework could build upon laws governing credit card and automatic teller machine transactions. It will also need to find ways of reducing the costs of transactions and must address the technological opportunities for new ways of creating stores of value (money). The acceptance and legal status of electronic payment systems will have a major impact on confidence and trust in e-commerce.

## **2.0 OBJECTIVES**

At the end of this unit, you should be able to:

- explain Internet banking
- state the characteristics of Internet banking
- state the activities associated with Internet banking
- process the auditing of Internet banking.

## **3.0 MAIN CONTENT**

### **3.1 Internet Banking Activities**

More and more banks are transforming their businesses by using Internet technology to develop or expand relationships with their customers. The extent to which the Internet is used in a bank depends on the relative maturity of the bank in regard to Internet technology. Banks offer Internet banking in two main ways. An existing bank with physical offices, ordinarily termed a brick-and-mortar bank, can establish a web site and offer Internet banking to its customers as an addition to its traditional delivery channels.

An alternative is to establish either a virtual, branchless or Internet-only bank. The computer server or bank database that lies at the heart of a virtual bank may be housed in an office that serves as the legal address of such a bank or at some other location. Virtual banks provide customers with the ability to make deposits and withdrawals via automated teller machines (ATMs) or through other remote delivery channels owned by other institutions.

Characteristics of Internet banking include:

- Unprecedented speed of change related to technological and customer service innovation,
- The ubiquitous and global nature of the Internet,

- The integration of Internet banking applications with legacy computer systems and
- The increasing dependence of banks on third parties that provide the necessary information technology.

Accordingly, a bank can perform Internet activities in one or more of these ways:

- **Informational**—This is the basic level of Internet banking. Typically, the bank has marketing information about the bank's products and services on a stand-alone server. Risks associated with these operations are relatively low, as informational systems typically have no path between the server and the bank's internal network. This level of Internet banking can be provided by the bank or can be outsourced. While the risk to a bank is relatively low, the data on the server or web site may be vulnerable to alteration. Appropriate controls, therefore, must be in place to prevent alterations of the data on the bank's server or web site.
- **Communicative**—This type of Internet banking system allows some interaction between the bank's systems and the customer. The interaction may be limited to electronic mail, accounts, loan applications or static file updates (name and address changes). Because these servers ordinarily have a direct path to the bank's internal networks, the operational risk is higher with this configuration than with informational systems. Controls should be in place to prevent, monitor and alert management of any unauthorised attempt to access the bank's internal networks and computer systems. Virus detection and prevention controls are also important in this environment.
- **Transactional**—This level of Internet banking allows customers to directly execute transactions with financial implications. There are two levels of transactional Internet banking, each with a different risk profile. The basic transactional site only allows a transfer of funds between the accounts of one customer and the bank. The advanced transactional site provides a means for generating payments directly to third parties outside of the bank. This can take the form of bill payments via a bank official check or electronic funds transfer/automated clearing house entries. Many banks are also offering payments from consumer to consumer using either payment method. When the transfers of funds are allowed to a point outside of the bank, the operational risk increases. Unauthorised access in this environment can lead or give rise to fraud. Since a communication path is typically complex and may include passing through several

public servers, lines or devices between the customer's and the bank's internal networks, this is the highest risk architecture and must have the strongest controls.

## **3.2 Review of Internet Banking**

### **3.2.1 Scope**

Banking, by its very nature, is a high-risk business. The major risks associated with banking activities are: strategic, reputation, operational (including security—sometimes called transactional—and legal risks), credit, price, foreign exchange, interest rate and liquidity. Internet banking activities do not raise risks that were not already identified in traditional banking, but it increases and modifies some of these traditional risks. The core business and the information technology environment are tightly coupled, thereby, influencing the overall risk profile of Internet banking. In particular, from the perspective of the IS auditor, the main issues are strategic, operational and reputation risk, as these are directly related to threats to reliable data flow and are heightened by the rapid introduction and underlying technological complexity of Internet banking. Banks should have a risk management process to enable them identify, measure, and control their technology risk exposure. Risk management of new technologies has three essential elements:

1. Risk management is the responsibility of the board of directors and senior management. They are responsible for developing the bank's business strategy and establishing an effective risk management methodology. They need to possess the knowledge and skills to manage the bank's use of Internet banking and all related risks. The board should make an explicit, informed and documented strategic decision as to whether and how the bank is to provide Internet banking services. The initial decision should include the specific accountabilities, policies and controls to address risks, including those arising in a cross-border context. The board should review, approve and monitor Internet banking technology-related projects that have a significant effect on the bank's risk profile and ensure that adequate controls are identified, planned and implemented.
2. Implementing technology is the responsibility of information technology senior management. They should have the skills to effectively evaluate Internet banking technologies and products, and to ensure that they are installed and documented appropriately. If the bank does not have the expertise to fulfill this responsibility internally, it should consider contracting with a

vendor who specialises in this type of business or engaging in an alliance with another third party with complementary technologies or expertise.

3. Measuring and monitoring risk is the responsibility of operational management. They should have the skills to effectively identify, measure, monitor and control risks associated with Internet banking. The board of directors should receive regular reports on the technologies employed, the risks assumed, and how those risks are managed.

Internal controls over Internet banking systems should be commensurate with the level of risk of the services the bank offers, the level of risk involved in the implementation and the bank's risk tolerance level. The review of internal control in Internet banking must help the IS auditor to provide reasonable assurance that the controls are appropriate and function appropriately. Control objectives for an individual bank's Internet banking technology and products might focus on:

- Consistency of technology planning and strategic goals, including effectiveness, efficiency and economy of operations and compliance with corporate policies and legal requirements
- Data and service availability, including business recovery planning
- Data integrity, including providing for safeguarding of assets, proper authorisation of transactions and reliability of the data flow
- Data confidentiality and privacy standards, including controls over access by both employees and customers
- Reliability of management reporting.

To appropriately evaluate the internal controls and their adequacy, the IS auditor should understand the bank's operational environment. *COBIT* (3<sup>rd</sup> ed.) published by the IT Governance Institute in 2000, has laid down seven information criteria to be met by information systems:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

The information criteria listed in are relevant in the case of Internet banking. Accordingly, a review of Internet banking should address how

the information criteria of COBIT are met by the Internet banking initiative/application/ implementation.

Compared with other forms/channels of banking activities, Internet banking depends greatly on the integrity or trust in the confidentiality of customer data and on the availability of the system. In this context, there should be in place, appropriate fall back options, as well as disaster recovery procedures. In the case of Internet banking involving payments or funds transfers, non-repudiation and integrity of the transactions are essential attributes. In such cases, the review of Internet banking should address the effectiveness of the Internet banking system controls in assuring non-repudiation and integrity. Due attention should be given to them while evaluating the availability of Internet banking solutions, especially if the continuity is based on cross-border processing, because it might infringe a regulation or might run counter to compliance with bank regulations.

It is essential in Internet banking to confirm that any communication, transaction or access request is legitimate. Accordingly, banks should use reliable methods for verifying the identity and authorisation of new customers as well as authenticating the identity and authorisation of established customers seeking to initiate electronic transactions. Customer verification during account origination is important to reduce the risk of theft, fraudulent transactions and money laundering activities. Strong customer identification and authentication processes are particularly important in the cross-border context given the difficulties that may arise from doing business electronically with customers across national and international borders, including the risk of identity impersonation and the difficulty in conducting effective credit checks on potential customers.

Auditing has more significance in the Internet banking environment, because a significant proportion of the transactions take place in paperless environments.

### **3.3 Independence**

#### **3.3.1 Professional Objectivity**

Before accepting the engagement, the IS auditor should provide reasonable assurance that any interests he/she may have in the Internet bank under review would not in any manner impair the objectivity of the review. In the event of any possible conflicts of interest, these should be explicitly communicated to the bank's management and the written approval of the bank's management should be obtained before accepting the assignment.



### 3.4 Competence

#### 3.4.1 Skills and Knowledge

The IS auditor should have the necessary technical and operational skills and knowledge to carry out the review of the technology employed and risks associated with Internet banking. The IS auditor should determine whether the technology and products are aligned with the bank's strategic goals. In particular, such reviews would call for bank operations knowledge and associated risks, knowledge of banking laws and regulations together with the technical knowledge necessary to evaluate aspects such as web hosting/web housing technologies, encryption technologies, network security architecture and security technologies, such as firewalls, intrusion detection and virus protection. Where expert advice or expert input is necessary, appropriate use should be made of external professional resources. The fact that external expert resources may be used should be communicated to the bank's management in writing.

### 3.5 Planning

#### 3.5.1 High-Level Risk Assessment

The IS auditor should gather information regarding the Internet banking objectives of the bank, the strategy used to achieve the objectives, the way that the bank is using Internet technology in the relationships with its customers (either informative, communicative or transactional, as set out in 3.0). The information thus gathered should be such that it helps in carrying out a high-level assessment of the banking risks as well as the risks pertaining to the information criteria of COBIT. This high-level risk assessment will help determine the scope and coverage of the review. If the bank has an enterprise risk framework, this can be used.

The IS auditor should follow a risk assessment approach for analysing and evaluating the main potential general and specific threats connected to implementation of Internet banking, the possible manifestations, the potential effect on the bank, the likelihood of occurrences and the possible risk management measures that can be implemented for preventing risks. The following **strategic risks** should be evaluated:

- The strategic assessment and risk analysis
- Integration within corporate strategic goals
- Selection and management of technological infrastructure
- Comprehensive process for managing outsourcing relationships with third-party providers

The following **security risks** should be evaluated:

- Customer security practices
- Authentication of customers
- Nonrepudiation and accountability of transactions
- Segregation of duties
- Authorisation controls within systems, databases and applications
- Internal or external fraud
- Data integrity of transactions, databases and records
- Audit trails for transactions
- Confidentiality of data during transmission
- Third-party security risk

The following **legal risks** should be evaluated:

- Disclosures of information to customers
- Privacy
- Compliance to laws, rules and statements of the regulator or supervisor
- Exposure to foreign jurisdictions

The following **reputation risks** should be evaluated:

- Service level delivery
- Level of customer care
- Business continuity and contingency planning

### 3.5.2 Scope and Objectivity of the Review

The IS auditor should, in consultation with the bank management where appropriate, clearly define the scope and objective of the review of Internet banking. The aspects to be covered by the review should be explicitly stated as part of the scope. The nature of the bank's Internet activities and volume of the Internet banking activities and the risks associated with them—as identified by the high-level risk assessment—dictate which aspects need to be reviewed as well as the extent and depth of the review.

For the purpose of the review, control objectives should be in accordance with regulations and applicable banking laws. The Internet is borderless, so it is easy for any bank using an Internet-based delivery channel to operate in a multi-state and even multi-country environment.

The bank may find itself bound by the laws, regulations and customs of wherever its customers are located rather than just where the bank is physically located. Therefore, the IS auditor should determine the geographic spread of the bank's current and planned customer base. The IS auditor needs to identify how many different jurisdictions have legal and regulatory control over the Internet banking operations and determine how the Internet bank is managing this risk.

### **3.5.3 Approach**

The IS auditor should formulate the approach in such a way that the scope and objectives of the review could be fulfilled in an objective and professional manner. The approach followed should depend on whether the review is a pre-implementation review or a post-implementation review. The approach should be appropriately documented. If the input or advice of external experts is to be used, this should also be specified as part of the approach.

### **3.5.4 Sign-off for the Plan**

Depending on the practices of the organisation, it may be appropriate for the IS auditor to obtain the agreement of the bank's management for the review plan and approach.

## **3.6 Performance of Internet Banking Review**

### **3.6.1 Execution**

The aspects to be reviewed and the review process should be chosen by taking into account the intended scope and objective of the review as well as the approach defined as part of the planning process.

In general, in gathering, analysing and interpreting the Internet banking environment, a study should be made of available documentation, such as bank regulations about Internet banking, Internet law, privacy law, web banking system documentation and use of the Internet banking solution.

To identify any problems relating to the Internet banking area which have been noted previously and which may require follow-up, the IS auditor should review the following documents:

- Previous examination reports
- Follow-up activities
- Work papers from previous examinations
- Internal and external audit reports

The IS auditor should map the key processes—both automated as well as manual—relating to the Internet banking initiative/ system.

The assessment of the core business risks should include a critical evaluation of the Internet banking objectives, strategy and business model.

The IS auditor should then assess the probability that the risks identified pertaining to these processes (business as well as IS risks) will materialise together with their likely effect, and document the risks along with the controls, which mitigate these risks.

As part of the IS risk assessment, external IS threats should be evaluated depending on the nature of products offered by a bank and the external threats to be addressed. These threats include denial of service, unauthorised access to data, unauthorised use of the computer equipment, which could arise from various sources such as casual hackers, competitors, alien governments, terrorists or disgruntled employees.

Depending on the nature of the pre- or post-implementation review, the IS auditor should test the significant processes in the test and or production environment to verify that the processes are functioning as intended. These tests include testing of balance inquiry, testing of bill presentation and payment and testing the security mechanisms using penetration testing.

In post implementation review the IS auditor should obtain at least, an understanding of network mapping, network routing, systems and network security assessment, and internal and external intrusion.

Since the Internet banking solution is predominantly an information technology solution, it should meet the information criteria established in COBIT, as well as other relevant standards or regulations of the industry. The extent of compliance with the information criteria, standards and/or regulations and the effect of noncompliance should be analysed.

### **3.6.2 Aspects to Review**

The following **organisation aspects** should be reviewed for whether:

- Due diligence and risk analysis are performed before the bank conducts Internet banking activities
- Due diligence and risk analysis are performed where cross-border activities are conducted

- Internet banking is consistent with the bank's overall mission, strategic goals and operating plans
- Internet application is compliant with the defined and approved business model
- Internet banking systems and/or services are managed in-house or outsourced to a third-party
- Management and personnel of the organisation display acceptable knowledge and technical skills to manage Internet banking
- Measures to ensure segregation of duties are in place
- Management reports are adequate to appropriately manage Internet banking transaction and payment service activities

The review should include **policy aspects** such as whether:

- Suitable policies have been defined and implemented regarding the acquisition of customers, the engagement of suppliers, the customers authentication, the privacy of customers/suppliers data, audit trail, the review of usage logs and whether the bank is keeping abreast of legal developments associated with Internet banking
- The bank is providing accurate privacy disclosures associated with its Internet banking product line
- Information is provided on the web site to allow customers to make informed judgment about the identity and regulatory status of the bank before they enter into Internet banking services (name of the bank and the location of its head office, the primary bank supervisory authority, ways to contact to customer service and other relevant information)
- The bank has established policies governing the use of hypertext links such that consumers can clearly distinguish between bank and non-bank products, and that they are informed when leaving the bank's web site
- There are appropriate procedures in place regarding change control, the review of audit trails and the review/analysis of usage logs (firewall logs and other reports)
- There are suitable and adequate procedures in place to ensure the privacy and integrity of the data and to ensure compliance with the applicable laws and regulations as well as best practice

The following **planning aspects** should be reviewed for whether:

- The planned information systems technology architecture is feasible and will result in safe and sound operations
- There are appropriate incident response plans in place to manage, contain and minimise problems arising from unexpected events, including internal or external attacks

- An “Internet product life cycle” exists and if it is followed both for developing, maintenance and upgrading Internet applications
- Business continuity and contingency plans for critical Internet banking processing and/or delivery systems are in place and regularly tested

The following **information systems infrastructure aspects** should be reviewed for whether:

- The infrastructure and systems are capable of expansion to accommodate the proposed business plan
- An information security architecture has been defined and is appropriate for the nature of the Internet banking model
- The bank has an adequate process and controls to address physical security for hardware, software and data communications equipment associated with the Internet banking system
- The bank has a sound process which ensures adequate control over the path between the web site and the bank’s internal networks or computer systems and whether the internal network is suitably protected from the external environment using appropriate firewall technology
- Databases and data flow are protected from unauthorised /inappropriate access
- There are suitable and adequate procedures in place to ensure the identification of access points and potential areas of vulnerability
- There are appropriate manual balancing controls where automated controls are inadequate
- The record for each customer transaction contains identification of the customer, the transaction number, the type of transaction, the transaction amount and other information of relevance, if it is stored and archived, for control purposes or other business functions such as marketing

The following **telecommunication infrastructure aspects** should be reviewed for whether:

- The network architecture is appropriate for the nature, timing and extent of the Internet banking operation
- The network protocols used are appropriate for the intended use (for instance, if payments or funds transfers are accepted through the Internet banking system, secure protocols should be used)
- The bank has an effective process to assess the adequacy of physical controls in place to restrict access to firewall servers and components
- Intrusion detection systems and virus control systems/procedures are in place

- There is adequate penetration testing of internal or external networks
- The communication across the network is made secure using virtual private network (VPN) and related encryption techniques where appropriate and necessary
- Adequate and strong encryption algorithms were selected to protect data during communication across the network

The following **authentication aspects** should be reviewed for whether:

- Control features are in place to validate the identity of prospective customers while they use the Internet to apply for new bank loan and/or deposit accounts
- Control features are built into the systems to ensure the authentication of the existing customer, the integrity of data and the confidentiality of transactions
- Authentication procedures are used to uniquely and positively identify the transacting party using digital certificates and digital signatures where necessary
- Nonrepudiation is ensured for an eventual later business or legal use where transactions are made using the Internet banking system
- The fault tolerance features of the Internet banking system are commensurate with the nature, volume and criticality of its system

The following **third-party service provider aspects** should be reviewed for whether:

- Due diligence review of the competency and financial viability was conducted prior to entering into any contract with third-party service providers
- The contracts with third-party service providers adequately protect the interests of the bank and the bank's customers, and whether the bank organisation has reviewed vendor contracts to ensure that the responsibilities of each party are appropriately identified and defined
- The bank organisation obtains and reviews internal or external audit reports of third-party service providers, evaluating vendor management processes or specific vendor relationships as they relate to information systems and technology, and whether all outsourced systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards
- The bank organisation has the right to conduct independent reviews and/or audits of security, internal control and business continuity and contingency plans of third-party service providers
- The security procedures of the third parties are appropriate and adequate where the Internet banking solution depends on the any third-party service providers such as Internet service providers (ISP),

certification authority (CA), registration authority (RA), web-hosting/housing agency

- Third-party service providers have appropriate business continuity and contingency plans for critical Internet banking processing and/or delivery systems are in place and regularly tested, and whether the bank receives copies of test result reports
- The bank has an adequate process to ensure that software maintained by the vendor is under a software escrow agreement and that the software is confirmed as being current on a regular basis where the bank obtains software products from a vendor
- A third –party’s opinion is sought in the pre-implementation phase of Internet applications for evaluating the security architecture solution that will be developed and configured

Where necessary and agreed with the bank, external expert input or advice should be used suitably in the collection, analysis and interpretation of the data.

The inferences and recommendations should be based on an objective analysis and interpretation of the data.

Appropriate audit trails should be maintained and protected for the data gathered, the analysis made and the inferences arrived at, as well as the corrective actions recommended.

Before finalising the report, the observations and recommendations should be validated with the stakeholders, board of directors and the bank’s management, as appropriate.

### **3.7 Reporting**

#### **3.7.1 Report Content**

The IS auditor should produce regular reports on the technologies employed, the risks assumed, and how those risks are managed. Monitoring system performance is a key success factor. Depending on the scope of its coverage, the report on Internet banking review carried out should address the following, as appropriate:

- The scope, objectives and methodology followed and assumptions
- An overall assessment of the Internet banking processes/systems solution in terms of key strengths and weaknesses as well as the likely effects of weaknesses
- Recommendations to overcome the significant weaknesses and to improve the Internet banking processes/systems solution



- A statement on the extent of compliance with bank regulations or applicable laws, along with the effect of any noncompliance
- A statement on the extent of compliance with the information criteria of COBIT, along with the effect of any noncompliance
- Recommendations regarding how the lessons of the review could be used to improve similar future solutions or initiatives

#### **4.0 CONCLUSION**

Internet banking as a form of electronic banking has carved out a niche for itself because it is global in nature. The attraction for Internet banking is the reduction in cost of operations, ease, speed and spread. This has brought attending challenges, especially security and fraud issues. For this purpose, detailed audit programmes and guidelines have been developed for Internet banking to forestall and minimise the potentials for fraud and abuse.

#### **5.0 SUMMARY**

- The term Internet banking refers to the use of the Internet as a remote delivery channel for banking services.
- More and more banks are transforming their businesses by using Internet technology to develop or expand relationships with their customers. The extent to which the Internet is used in a bank depends on the relative maturity of the bank in regard to Internet technology
- Banking, by its very nature, is a high-risk business. The major risks associated with banking activities are: strategic, reputation, operational (including security—sometimes called transactional—and legal risks), credit, price, foreign exchange, interest rate and liquidity.
- Internal controls over Internet banking systems should be commensurate with the level of risk of the services the bank offers, the level of risk involved in the implementation and the bank's risk tolerance level.
- Before accepting the engagement, the IS auditor should provide reasonable assurance that any interests he/she may have in the Internet bank under review would not in any manner impair the objectivity of the review
- The IS auditor should have the necessary technical and operational skills and knowledge to carry out the review of the technology employed and risks associated with Internet banking

- In general, in gathering, analysing and interpreting the Internet banking environment, a study should be made of available documentation, such as bank regulations about Internet banking, Internet law, privacy law, web banking system documentation and use of the Internet banking solution.
- Due diligence and risk analysis are performed before the bank conducts Internet banking activities
- Suitable policies have been defined and implemented regarding the acquisition of customers, the engagement of suppliers, the customers authentication, the privacy of customers/suppliers data, audit trail, the review of usage logs and whether the bank is keeping abreast of legal developments associated with Internet banking
- Appropriate audit trails should be maintained and protected for the data gathered, the analysis made and the inferences arrived at, as well as the corrective actions recommended.

## 6.0 TUTOR–MARKED ASSIGNMENT

1. Mention five **control objectives** for an individual bank's Internet banking technology and products.
2. In the planning phase of an Internet banking audit, list ten security risks to be checked.

## 7.0 REFERENCES/FURTHER READINGS

Federal Reserve Bank of Chicago, USA. *An Internet Banking Primer*.

Basel Committee on Banking Supervision, May (2001). *Basle Directive N° 82, Risk Management Principles for Electronic Banking*. Switzerland.

Basel Committee on Banking Supervision May (2001). *Basle Directive N° 86, Sound Practices for the Management and Supervision of Operational Risk*. Switzerland.

Basel Committee on Banking Supervision, July (2002). *Basle Directive N° 91, Risk Management Principles for Electronic Banking*. Switzerland.

Monetary and Economic Department, Bank for International Settlements, November (2001). *BIS Papers N° 7. Electron Finance: A New Perspective and Challenges*. Switzerland.

Cronin, Mary J. *Banking and Finance on the Internet*. USA: John Wiley & Sons, Inc.

Essinger, James, *The Virtual Banking Revolution*. United Kingdom: Thomson Business Press.

Comptroller of the Currency Administrator of National Banks, October (1999). *Internet Banking Comptroller's Handbook*. USA.

Furst, Karen, William W. Lang & Daniel, E. Nolle (2000). "Internet Banking: Developments and Prospects". Economic and Policy Analysis Working Paper 2000-9. Office of the Comptroller of the Currency, September 2000, USA.

Comptroller of the Currency Administrator of National Banks, January (2001). *The Internet and the National Bank Charter*. USA.

## **UNIT 4      ELECTRONIC FRAUD (1) *INTERNET FRAUD***

### **CONTENTS**

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
  - 3.1 Geographic Origin
  - 3.2 Popular Products
  - 3.3 Identity Theft Schemes
  - 3.4 Purchase Scams
  - 3.5 Online Automotive Fraud
  - 3.6 Cash the Check System
  - 3.7 Re-Shippers
  - 3.8 Call Tag Scam
  - 3.9 Business Opportunity/ “Work-at-Home” Schemes
  - 3.10 Website Scams
  - 3.11 International Modem Dialing
  - 3.12 Phishing
  - 3.13 Pharming
  - 3.14 Auction and Retail Schemes Online
  - 3.15 Stock Market Manipulation Schemes
    - 3.15.1 Pump-and-Dump Schemes
    - 3.15.2 Short-Selling or “Scalping” Schemes
  - 3.16 Avoiding Internet Investment Scams
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 70. References/Further Readings

### **1.0 INTRODUCTION**

The term “Internet fraud” generally refers to any type of fraud scheme that uses one or more online services - such as chat rooms, e-mail, message boards, or web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Internet fraud is committed in several ways. The FBI and police agencies worldwide have people assigned to combat this type of fraud; according to figures from the FBI, U.S., companies' losses due to Internet fraud in 2003 surpassed US\$500 million. In some cases, fictitious merchants advertise goods for very low prices and never deliver. However, that type of fraud is minuscule compared to criminals using stolen credit card information to buy goods and services.

The Internet serves as an excellent tool for investors, allowing them to easily and inexpensively research investment opportunities. But the Internet is also an excellent tool for fraudsters.

## **2.0 OBJECTIVES**

At the end of this unit, you should be able to:

- explain Internet fraud and its origin
- identify types of Internet fraud
- identify some Internet fraud schemes
- explain how to avoid and escape Internet fraud.

## **3.0 MAIN CONTENT**

### **3.1 Geographic Origin**

In some cases Internet fraud schemes originate in the US and European countries, but a significant proportion seems to come from Africa, particularly Nigeria, and sometimes from Ghana and Egypt. Some originate in Eastern Europe, Southwest Asia and China. For some reason, many fraudulent orders seem to originate from Belgium, from Amsterdam in the Netherlands, from Norway, and from Malmö in Sweden.

### **3.2 Popular Products**

Fraudsters seem to prefer small and valuable products, such as: watches, jewelry, laptops, digital cameras, and camcorders. These items are usually commodities that are easily sellable and have a broad range of appeal. However, fraud in hosted marketplaces such as Ebay covers a broad range of products from cellular phones to desktop computers. The craft has continually evolved in sophistication. In some instances, a picture of the product is sent in place of the actual product. Other times, products are outright never sent after the bill is charged to credit card accounts. Victims are left to deal with credit card companies for chargebacks.

### **3.3 Identity Theft Schemes**

#### **1. Stolen Credit Cards**

Most Internet fraud is done through the use of stolen credit card information which is obtained in many ways, the simplest being copying information from retailers, either online or offline. There have been many cases of hackers obtaining huge quantities of credit card

information from companies' databases. There have been cases of employees of companies that deal with millions of customers in which they were selling the credit card information to criminals.

Despite the claims of the credit card industry and various merchants, using credit cards for online purchases can be insecure and carry a certain risk. Even so called "secure transactions" are not fully secure, since the information needs to be decrypted to plain text in order to process it. This is one of the points where credit card information is typically stolen.

## **2. Wire Transfer Info**

Some fraudsters approach merchants asking them for large quotes. After they quickly accept the merchant's quote, they ask for wire transfer information to send payment. Immediately, they use online check issuing systems as Qchex that require nothing but a working email, to produce checks that they use to pay other merchants or simply send associates to cash them.

## **3.4 Purchase Scams**

### **1. Direct Solicitation**

The most straightforward type of purchase scam is a buyer in another country approaching many merchants through spamming them and directly asking them if they can ship to them using credit cards to pay.

Most likely, a few weeks or months after the merchant ships and charges the fake credit card, he/she will be hit with a chargeback from the credit card processor and lose all the money.

### **2. Counterfeit Postal Money Order**

According to the FBI and postal inspectors, there has been a significant surge in the use of Counterfeit Postal Money Orders since October 2004. More than 3,700 counterfeit postal money orders (CPMOs) were intercepted by authorities from October to December of 2004, and according to the USPS, the "quality" of the counterfeits is so good that ordinary consumers can easily be fooled.

On March 9, 2005, the FDIC issued an alert [\[1\]](#) stating that it had learned that counterfeit U.S. postal money orders had been presented for payment at financial institutions.

On April 26, 2005, Tom Zeller Jr. wrote an article in *The New York Times* regarding a surge in the quantity and quality of the forging of U.S. postal money orders, and its use to commit online fraud. The article shows a picture of a man that had been corresponding with a woman in Nigeria through a dating site, and received several fake postal money orders after the woman asked him to buy a computer and mail it to her.

Who has received counterfeit postal money orders (CPMOs)?:

- Small Internet retailers
- Classified advertisers
- Individuals that have been contacted through email or chat rooms by fraudsters posing as prospective social interests or business partners, and convinced to help the fraudsters unknowingly.

The penalty for making or using counterfeit postal money orders is up to ten years in jail and a US\$25,000 fine.

### **3.5 Online Automotive Fraud**

There are two basic schemes in online automotive fraud:

1. A fraudster posts a vehicle for sale on an online site, generally for luxury or sports cars advertised for thousands less than market value. The details of the vehicle, including photos and description, are typically lifted from sites such as eBay Motors and re-posted elsewhere. An interested buyer, hopeful for a bargain, emails the seller, who responds saying the car is still available but is located overseas. He then instructs the buyer to send a deposit via wire transfer to initiate the “shipping” process. The unwitting buyer wires the funds, and doesn't discover until days or weeks later that they were scammed
2. A fraudster feigns interest in an actual vehicle for sale on the Internet. The “buyer” explains that a client of his is interested in the car, but due to an earlier sale that fell through has a certified check for thousands more than the asking price and requests the seller to send the balance via wire transfer. If the seller agrees to the transaction, the buyer sends the certified check via express courier. The seller takes the check to their bank, which makes the funds available immediately. Thinking the bank has cleared the check, the seller follows through on the transaction by wiring the balance to the buyer. Days later, the check bounces and the seller realises they have been scammed. But the money has long since been picked up and is not recoverable.

In another type of fraud, a fraudster contacts the seller of an automobile, asking for the vehicle identification number, putatively to check the accident record of the vehicle. However, the supposed buyer actually uses the VIN to make fake papers for a stolen car that is then sold.

### **3.6 Cash the Check System**

In some cases, fraudsters approach merchants and ask for large orders: \$50,000 to \$200,000, and agree to pay via wire transfer in advance. After brief negotiation, the buyers give an excuse about the impossibility of sending a bank wire transfer. The buyer then offers to send a check, stating that the merchant can wait for the check to clear before shipping any goods. The check received, however, is a counterfeit of a check from a medium to large company in US. If asked, the buyer will claim that the check is money owed from the large company. The merchant deposits the check and it clears, so the goods are sent. Only later, when the larger company notices the check, will the merchant's account be debited.

In some cases, the fraudsters agree to the wire but ask the merchant for their bank's address. The fraudsters send the counterfeited check directly to the merchant's bank with a note asking to deposit it to the merchant's account. Unsuspecting bank officers deposit the check, and then the fraudster contacts the merchant stating that they made a direct deposit into the merchant's account.

### **3.7 Re-Shippers**

Re-shipping scams trick individuals or small businesses into shipping goods to countries with weak legal systems. The goods are generally paid for with stolen or fake credit cards.

#### **Version 1**

In this version, the fraudsters have armies of people actively recruiting single women from Western countries through chat & matchmaking sites. At some point, the criminal promises to marry the lady and come to their home country in the near future. Using some excuse the criminal asks permission of his "future wife" to ship some goods he is going to buy before he comes. As soon as the woman accepts the fraudster uses several credit cards to buy at different Internet sites simultaneously. In many cases the correct billing address of the cardholder is used, but the shipping address is the home of the unsuspecting "future wife". Around the time when the packages arrive, the criminal invents an excuse for not coming and tells his "bride" that he urgently needs to pick up most or all the packages. Since the woman has not spent any money, she sees



nothing wrong and agrees. Soon after, she receives a package delivery company package with pre-printed labels that she has agreed to apply to the boxes that she already has at home. The next day, all boxes are picked up by the package delivery company and shipped to the criminal's real address. After that day the unsuspecting victim stops receiving communications from the "future husband" because her usefulness is over. To make matters worse, in most cases the criminals were able to create accounts with the package deliverer, based on the woman's name and address. So, a week or two later, the woman receives a huge freight bill from the shipping company which she is supposed to pay because the goods were shipped from her home. Unwittingly, the woman became the criminal re-shipper and helped him with his criminal actions.

### **Version 2**

This is a variant of Version 1, in which criminals recruit people through classified advertising. The criminals present themselves as a growing European company trying to establish a presence in the U.S. and agree to pay whatever the job applicant is looking to make, and more. The fraudsters explain to the unsuspecting victim that they will buy certain goods in the U.S. which need to be re-shipped to a final destination in Europe. When everything is agreed they start shipping goods to the re-shipper's house. The rest is similar to the Version 1. Sometimes, when the criminals send the labels to be applied to the boxes, they also include a fake cheque, as payment for the re-shipper's services. By the time the cheque bounces unpaid, the boxes have been picked up already and all communication between fraudster and re-shipper has stopped.

### **Version 3**

This is a variant of the Version 2, in which criminals recruit people through spam. The criminals present themselves as a growing Chinese company trying to establish a presence in the U.S. or Europe and agree to pay an agent whatever the unsuspecting victim is looking to make, and more. Here is an example of a recruiting email.

*Dear Sir/Madam, I am Mr. XXX XXX, managining XXXXXXXXXXXX Corp. We are a company who deal on mechanical equipment, hardware and minerals, electrical products, Medical & Chemicals, light industrial products and office equipment, and export into the Canada/America and Europe. We are searching for representatives who can help us establish a medium of getting to our costumers in the Canada/America and Europe as well as making payments through you to us. Please if you are interested in transacting business with us we will be glad. Please contact us for more information. Subject to your satisfaction you will be*

*given the opportunity to negotiate your mode of which we will pay for your services as our representative in Canada/America and Europe. Please if you are interested forward to us your phone number/fax and your full contact addresses. Thanks in advance. Mr. XXX XXX. Managing Director"*

### **3.8 Call tag Scam**

The Merchant Risk Council reported that the "call tag" scam re-emerged over the 2005 holidays and several large merchants suffered losses. Under the scheme, criminals use stolen credit card information to purchase goods online for shipment to the legitimate cardholder. When the item is shipped and the criminal receives tracking information via email, he/she calls the cardholder and falsely identifies himself as the merchant that shipped the goods, saying that the product was mistakenly shipped and asking permission to pick it up upon receipt. The criminal then arranges the pickup issuing a "call tag" with a shipping company different than the one the original merchant used. The cardholder normally doesn't notice that there is a second shipping company picking up the product, which in turn has no knowledge it is participating in a fraud scheme. The cardholder then notices a charge on his card and generates a chargeback to the unsuspecting merchant.

### **3.9 Business Opportunity/ "Work-at-Home" Schemes**

Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in "work-at-home" ventures. These schemes typically require the individuals to pay anywhere from \$35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

Often, after paying a registration fee, the applicant will be sent advice on how to place ads similar to the one that recruited him in order to recruit others, which is effectively a pyramid scheme.

Other types of work at home scams include home assembly kits. The applicant pays a fee for the kit, but after assembling and returning the item, it's rejected as sub-standard, meaning the applicant is out of pocket for the materials. Similar scams include home-working directories, medical billing, data entry at home or reading books for money.

### **3.10 Website Scams**

#### **Click Fraud**

The latest scam to hit the headlines is the multi-million dollar Clickfraud which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via Spyware, the affiliate is then paid a commission on the cost-per-click that was artificially generated. Affiliate programmes such as Google's AdSense capability pay high commissions that drive the generation of bogus clicks. With paid clicks costing as much as \$100 and an online advertising industry worth more than \$10 Billion, this form of Internet fraud is on the increase.

#### **Another form of Click Fraud**

This type of fraud involves a supposed internet marketing specialist presenting a prospective client with detailed graphs and charts that indicate that his web site receives (x) thousands of hits per month, emphasising that if you pay for his services you will succeed in getting a number clicks converted to customers or clients.

When you receive no request for more information and no clients, the fraudster responds that it must be something your web site is not doing right.

One recent experience resulted in the discovery that this fraudster's website had 176,000 pages, all with the same or very similar pages, the keywords included the days of the week and the months of the year, but nothing to do with any business except the fraudster's details. The experience resulted in the loss of £950 --English pounds equivalent to US\$1860.

### **3.11 International Modern Dialing**

Many consumers connect to the Internet using a modem calling a local telephone number. Some web sites, normally containing adult content, use international dialing to trick consumers into paying to view content on their web site. Often these sites purport to be free and advertise that no credit card is needed. They then prompt the user to download a "viewer" or "dialer" to allow them to view the content. Once the programme is downloaded it disconnects the computer from the Internet and proceeds to dial an international long distance or premium rate number, charging anything up to US\$7-8 per minute. An international block is recommended to prevent this, but in the U.S. and Canada, calls to the Caribbean (except Haiti) can be dialed with a "1" and a three-digit

area code, so such numbers, as well as “10-10 dial-round” phone company prefixes, can circumvent an international block.

### 3.12 Phishing

“Phishing” is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message). It is a form of social engineering attack.

The term was coined in the mid 1990s by crackers attempting to steal AOL accounts. An attacker would pose as an AOL staff member and send an instant message to a potential victim. The message would ask the victim to reveal his or her password, for instance to “verify your account” or to “confirm billing information”. Once the victim gave over the password, the attacker could access the victim's account and use it for criminal purposes, such as spamming.

Phishing has been widely used by fraudsters using spam messages masquerading as large banks (Citibank, Bank of America) or PayPal. These fraudsters can copy the code and graphics from legitimate websites and use them on their own sites to create a legitimate- looking scam web page. They can also link to the graphics on the legitimate sites to use on their own scam site. These pages are so well done that most people cannot tell that they have navigated to a scam site. Fraudsters will also put the text of a link to a legitimate site in an e-mail but use the source code to links to own fake site. This can be revealed by using the “view source” feature in the e-mail application to look at the destination of the link or putting the cursor over the link and looking at the code in the status bar of the browser. Although many people don't fall for it, the small percentage of people that do fall for it, multiplied by the sheer numbers of spam messages sent, presents the fraudster with a substantial incentive to keep doing it.

### 3.13 Pharming

**Pharming** is the exploitation of vulnerability in the DNS server software that allows a hacker to acquire the domain name for a site, and to redirect that website's traffic to another web site. DNS servers are the machines responsible for resolving internet names into their real addresses - the “signposts” of the Internet.

If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to “phish” or steal a computer user's passwords, PIN or account number. Note that this is only possible when

the original site was not SSL protected, or when the user is ignoring warnings about invalid server certificates.

For example, in January 2005, the domain name for a large New York ISP, Panix, was hijacked to a site in Australia. In 2004 a German teenager hijacked the eBay.de domain name. Secure e-mail provider Hushmail was also caught by this attack on 24th of April 2005 when the attacker rang up the domain registrar and gained enough information to redirect users to a defaced webpage.

### **3.14 Auction and Retail Schemes Online**

Fraudsters launch auctions on eBay or TradeMe with very low prices and no reservations especially for high priced items like watches, computers or high value collectibles. They received payment but never deliver, or deliver an item that is less valuable than the one offered, such as counterfeit, refurbished or used. Some fraudsters also create complete webstores that appear to be legitimate, but they never deliver the goods. In some cases, some stores or auctioneers are legitimate but eventually they stopped shipping after cashing the customers' payments.

Sometimes fraudsters will combine phishing to hijacking legitimate member accounts on eBay, typically with very high numbers of positive feedback, and then set up a phony online store. They received payment usually via check, money-order, cash or wire transfer but never deliver the goods; and then they leave the poor, unknowing eBay member to sort out the mess. In this case the fraudster collects the money while ruining the reputation of the conned eBay member and leaving a large number of people without the goods they thought they purchased.

### **3.15 Stock Market Manipulation Schemes**

These are also called investment schemes online. Criminals use these to try to manipulate securities prices on the market, for their personal profit. According to enforcement officials of the Securities and Exchange Commission, the two main methods used by these criminals are.

#### **3.15.1 Pump-and-Dump Schemes**

False and/or fraudulent information is disseminated in chat rooms, forums, internet boards and via email (spamming), with the purpose of causing a dramatic price increase in thinly traded stocks or stocks of shell companies (the "pump"). As soon as the price reaches a certain level, criminals immediately sell off their holdings of those stocks (the "dump"), realising substantial profits before the stock price falls back to

its usual low level. Any buyers of the stock who are unaware of the fraud become victims once the price falls. When they realise the fraud, it is too late to sell. They lost a high percentage of their money. Even if the stock value does increase, the stocks may be hard to sell because of lack of interested buyers, leaving the shareholder with the shares for a far longer term than desired.

### **3.15.2 Short-Selling or “Scalping” Schemes**

This scheme takes a similar approach to the "pump-and-dump" scheme, by disseminating false or fraudulent information through chat rooms, forums, Internet boards and via email (spamming), but this time with the purpose of causing dramatic price decreases in a specific company's stock. Once the stock reaches a certain low level, criminals buy the stock or options on the stock, and then reverse the false information or just wait for it to wear off with time or to be disproved by the company or the media. Once the stock goes back to its normal level, the criminal sells the stock or option and reaps the huge gain.

### **3.16 Avoiding Internet investment Scams**

The US Security Exchange Commission has enumerated guideline on how to avoid Internet investment scams. The summary is as follows:

- The Internet allows individuals or companies to communicate with a large audience without spending a lot of time, effort, or money. Anyone can reach tens of thousands of people by building an Internet web site, posting a message on an online bulletin board, entering a discussion in a live "chat" room, or sending mass e-mails.
- If you want to invest wisely and steer clear of frauds, you must get the facts.
- The types of investment fraud seen online mirror the frauds perpetrated over the phone or through the mail. Consider all offers with skepticism.

## **4.0 CONCLUSION**

The forms of fraud associated with the Internet are so numerous and of different backgrounds making it the more difficult to keep accurate track of them. These fraud schemes are threatening the good purposes and potentials associated with the Internet. However, concerted efforts are equally made by relevant agencies to keep track of these fraud schemes and minimise their effects on the Internet technology.

## **5.0 SUMMARY**

- The term **Internet fraud** generally refers to any type of fraud scheme that uses one or more online services - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.
- In some cases Internet fraud schemes originate in the US and European countries, but a significant proportion seems to come from Africa, particularly Nigeria, and sometimes from Ghana and Egypt.
- Fraudsters seem to prefer small and valuable products, such as: watches, jewelry, laptops, digital cameras, and camcorders.
- Most Internet fraud is done through the use of stolen credit card information which is obtained in many ways, the simplest being copying information from retailers, either online or offline.
- The most straightforward type of purchase scam is a buyer in another country approaching many merchants through spamming them and directly asking them if they can ship to them using credit cards to pay.
- In another type of fraud, a fraudster contacts the seller of an automobile, asking for the vehicle identification number, putatively to check the accident record of the vehicle.
- Re-shipping scams trick individuals or small businesses into shipping goods to countries with weak legal systems. The goods are generally paid for with stolen or fake credit cards.
- The Merchant Risk Council reported that the “call tag” scam re-emerged over the 2005 holidays and several large merchants suffered losses
- The latest scam to hit the headlines is the multi-million dollar Clickfraud which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via Spyware, the affiliate is then paid a commission on the cost-per-click that was artificially generated.
- Many consumers connect to the Internet using a modem calling a local telephone number
- “Phishing” is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message
- **Pharming** is the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the domain name for a site, and to redirect that website's traffic to another web site
- Fraudsters launch auctions on eBay or TradeMe with very low prices and no reservations especially for high priced items like watches, computers or high value collectibles.

- The US Security Exchange Commission has enumerated guidelines on how to avoid Internet investment scams.

## **6.0 TUTOR–MARKED ASSIGNMENT**

1. List ten types of Internet frauds and scams.
2. Briefly discuss how to avoid Internet investment scam and fraud.

## **7.0 REFERENCES/FURTHER READINGS**

Counterfeit U.S. Postal Money Orders Counterfeit Postal Money Orders are Reportedly in Circulation (*FDIC*) March 9, 2005.

A Common Currency for Online Fraud Forgers of U.S. Postal Money Orders Grow By Tom Zeller Jr (*NYT*) April 26, 2005.

## **UNIT 5 ELECTRONIC FRAUD (2) *ADVANCE FEE FRAUD***

### **CONTENTS**



- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
  - 3.1 History
  - 3.2 Implementation
  - 3.3 Suspicious Signs in E-mails
  - 3.4 Variants
    - 3.4.1 Invitation to Visit the Country
    - 3.4.2 Credit Card Use through IP Relay
    - 3.4.3 Romance Angle
    - 3.4.4 Auction Overpayment, Fake Check
    - 3.4.5 False Escrow
    - 3.4.6 Hitman
    - 3.4.7 eBay/Western Union Scam
    - 3.4.8 Lottery Scam
    - 3.4.9 Inheritance Scam
    - 3.4.10 False Online Storefront Scam
    - 3.4.11 Classified Advertisement Scams
    - 3.4.12 Tutor Scams
    - 3.4.13 Escort Scams
    - 3.4.14 Black Money Scams
    - 3.4.15 Rental Scams
    - 3.4.16 Puppy Scams
  - 3.5 Consequences
    - 3.5.1 Monetary Loss Estimates
    - 3.5.2 Physical Harm or Death
    - 3.5.3 Kidnapping
    - 3.5.4 Murder
    - 3.5.5 Arrests
    - 3.5.6 The Victim Becomes a Criminal
    - 3.5.7 Impede E-Mail Output
  - 3.6 Proposed Legislation
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

## **1.0 INTRODUCTION**

An **advance fee fraud** is a confidence trick in which the target is persuaded to advance relatively small sums of money in the hope of realising a much larger gain.

## 2.0 OBJECTIVES

At the end of this unit, you should be able to:

- explain advance fee fraud and its origin
- explain tail signs of advance fee fraud
- identify different forms of advance fee fraud.

## 3.0 MAIN CONTENT

### 3.1 History

The 419 scam originated in the early 1990s as the oil-based economy of Nigeria went downhill. Several unemployed university students first used this scam as a means of manipulating business visitors interested in shady deals in the Nigerian oil sector before targeting businessmen in the West, and later the wider population. Early variants were often sent via letters, fax, or even telex. The spread of email and easy access to email harvesting software made the cost of sending scam letters through the Internet extremely cheap. In reality it has often been linked to small organised gangs, who often work together, both in Western cities and in developing nations. In recent years, the 419 scam has spurred imitations from other locations in Africa and Eastern Europe.

The number “419” refers to the article of the Nigerian Criminal Code (part of Chapter 38: “Obtaining Property by false pretences; Cheating”) dealing with fraud. The American Dialect Society has traced the term “419 fraud” back to 1992.

The advance fee fraud is a derivation of a much older scam dating back to 1588 in the form of a Spanish Prisoner scam. The fictitious prisoner would promise to share non-existent treasure with the person who would send them money to bribe their guards.

### 3.2 Implementation

The “investors” are contacted, typically with an offer of the type “A rich person from the needy country needs to discreetly move money abroad, would it be possible to use your account?”. The sums involved are usually in the millions of dollars, and the investor is promised a large share, often forty percent. The proposed deal is often presented as a “harmless” white-collar crime, in order to dissuade participants from

later contacting the authorities. Similarly, the money is often said to be the embezzled funds of a recently deposed or killed dictator. The operation is professionally organised in Nigeria, with offices, working fax numbers, and often contacts at government offices. The investor who attempts to research the background of the offer will often find that all pieces fit perfectly together.

If they then agree to the deal, the other side will first send several documents bearing official government stamps; seals etc., and then introduce delays, such as “in order to transmit the money, we need to bribe a bank official. Could you help us with a loan?” or “In order for you to be allowed to be a party to the transaction, you need to have holdings at a bank of \$100,000 or more”. More delays and more additional costs are added, always keeping the promise of an imminent large transfer alive. Sometimes psychological pressure is added by claiming that the fraudster side, in order to pay certain fees, had to sell all belongings and borrow money on their houses or by pointing out the different salary scale and living conditions in Africa compared to the West. Most of the time, however, the needed psychological pressure is self-applied; once the victim has put money in toward the payoff, they feel they have a vested interest in seeing the “deal” through.

In any case, the promised money transfer never happens. The money or gold does not exist. Such spam is often sent from Internet cafes equipped with satellite Internet. Recipient addresses and email content are copied and pasted into a web mail interface using a standalone storage medium, such as a memory card.

Some London-based gangs have been known to use spamware on laptops which they surreptitiously connect to the café's network, but even this software is notably out-of-date. While this method is significantly more labour-intensive per mail sent than others, it offers near-total anonymity and allows them to very quickly and easily relocate. The often very professional layout of web pages and so on used in the scams suggests that they do not lack technical sophistication.

### **3.3 Suspicious Signs in Emails**

As well as the email subject or contents, there are often some clear signs that 419 scam emails contain which should alert a recipient to be suspicious.

- **"Name Dropping"** - the naming of a reputable business, government body, or bank, or the description of some event which is reported in a reputable online newspaper. Often a link will be

provided to a newspaper report on the death of a supposed bank account holder, or the arrest of a supposed family member.

- **Inappropriate Contact** - for example, a lottery win may be emailed by a person claiming to work in a bank. Or, the sender claims to be a lawyer but the email address does not look like one written by a member of the legal establishment.
- **Mobile Phone Numbers** - the contact numbers will be cell (mobile) phones, or fax, not landline. In the UK, such numbers start with +44-7, 07- or 7-, although with public VOIP services increasingly available in major financial centres, use of apparently land line numbers (+44-20 for London) is on the rise.
- **Free Email Accounts** - the reply-to email address will often not match the company claimed. Thus a person may claim to be writing from HSBC (a major bank) but the email address used is a free Hotmail or Yahoo! account. Scammers will sometimes attempt to forestall this criticism by saying they are using their "private" email address so their "bosses" will not discover the plan.
- **Unearned Praise** - the email, from a complete stranger, almost always speaks of the recipient's reputation for honesty, integrity, and above all else discretion. The praise would be strong if it were not coming from a complete stranger.
- **Poor English** - despite the supposed formal titles (diplomats and bankers are frequent), emails sent by such scammers will often clearly reflect an inability to write in proper English; serious spelling and grammar mistakes are quite common.

### 3.4 Variants

#### 3.4.1 Invitation to Visit the Country

Sometimes, victims are invited to a country to meet real or fake government officials. Some victims who do travel are instead held for ransom. In some rumoured cases they are smuggled into the country without a visa and then threatened into giving up more money, as the penalties for being in a foreign country without a visa are severe. In the most extreme cases the victim has even been murdered.

#### 3.4.2 Credit Card Use through IP Relay

In another variation of the scam, the scammer places calls through IP Relay, a US federally funded Internet telerelay service for deaf/hard of hearing/speech-disabled individuals. The scammer calls various businesses, attempting to purchase items with stolen or fraudulent credit cards. Often, individuals are targeted as well, most of whom have advertised a product or service online.

Typically, in an IP-Relay scam call, the scammer will place several calls using a relay operator. Calling to businesses or private parties, the scammer will inquire about merchandise/services offered, and then immediately and with few questions asked, attempt to purchase the merchandise. The scammer (referred to as *guyman*) then proceeds to ask the potential victim (known in Nigeria as a *mugu*; a Lagos pidgin word for "fool") for an e-mail address, by which he can contact the victim to proceed with the closing of the fraudulent transaction.

The scammer proceeds to send the victim a counterfeit cheque or money order, with instructions requiring that it be cashed, and that excess funds be sent back to the scammer (advance fee fraud). When it is determined by the authorities that the money order is counterfeit, the victim is usually arrested and charged with various offenses relating to the scam. Credit-card fraud is not the only kind of fraud reported through IP Relay. A relay scammer typically will use IP Relay for all fraud-related transactions/telephone calls within the United States.

Often a scammer will browse through online classified ads (such as craigslist.org) and will use the IP Relay service to contact sellers to make inquiries about the item listed in the ad. Most commonly the scammers target persons whose ads advertise live animals (i.e. puppies), automobiles, high-dollar electronic devices, etc. In this scenario, the scammer sends the seller a cheque for the advertised item with an overpayment-- the victim is given instructions to cash the cheque or money-order and to wire the remaining balance via Western Union or Moneygram. The victim is at a loss in this situation when the authorities discover the cheque/money order is not legitimate.

Because of current FCC regulations and confidentiality laws, operators are required to relay every call verbatim and must adhere to a strict code of confidentiality and ethics. Thus no relay operator is permitted to make judgments about the legality and/or legitimacy of any relay call and must relay the call without interference. As such, the relay operator cannot warn victims even when they suspect that the call is a scam; some sources claim that up to half of all IP Relay calls are scams.

Some IP Relay companies have certain fraud criteria in which a supervisor is able to come on the line and inform the person that has been called that the call "fits a pattern of fraudulent and illegal activity".

It is then up to the voice person whether he or she wishes to continue the call.

### **3.4.3 Romance Angle**

A recent variant is the “Romance Scam” which is a money-for-romance angle. The victim is usually approached on an online dating service and becomes interested in a “lady” or “man” who has attractive pictures posted, generally stolen from online portfolios of modeling agencies. The offending party claims to be interested in meeting the victim, but needs some cash up front in order to book the plane, hotel room, and other expenses. In other cases he or she may have just travelled to a country (for tourism or business) and has been arrested by corrupt officials, stranded at a hotel, has money orders (which are counterfeit) that can't be cashed, or become ill from eating the local food, and needs an emergency wire transfer to bail or bribe his/her way out. As with other variants, money always seems to travel to Africa mainly via Western Union, and the "lady" or "man" always seems to come up with additional reasons for requesting more funds. This version of the scam is, at its core, identical to the classic Spanish Prisoner con, which dates back to the Renaissance.

### **3.4.4 Auction Overpayment, Fake Check**

A car that the prospective victim advertised on eBay, for example, a legitimate classified-ads website such as Craig's list by official, certified, bank or cashier's check. The check will have an "accidentally" or mutually agreed higher value than the price of the item, so the scammer asks the victim to wire the extra money to some third party as soon as the check clears. Because banks in the USA are required by law to honor a check within 1-5 working days (even before a check has cleared), they will report the proceeds as available for withdrawal before the check is presented to the issuing bank for clearance and the fraud is discovered. Most banks will hold the victim accountable for the value of the counterfeit check.

There is a simple way to avoid many instances of eBay auction overpayment fraud. The scammer usually or always wants to buy the merchandise immediately, so if the auction offers a "Buy It Now" option, the scammer will use it to end the auction, request shipping, and offer the overpayment. Therefore, if the seller avoids offering "Buy It Now," the scammer will be able only to send the seller a message requesting to buy the item immediately for an overpayment. The seller can then deny (or simply ignore) the request. This type of scam tends to target laptop computers, for obvious reasons. If a seller's auction is ended by someone clicking Buy It Now, there is still a way to detect

scamming. The buyer will ask the seller to ship to a different address. The buyer will hide the address until he/she sends the seller a shipping label to print. The shipping label's information will reveal a faraway address--often in Lagos, Nigeria--that the seller may not have wanted to ship to.

A variation on the eBay scam involves sending a request for payment for an item that the alleged seller does not own but claims to have sent. Since actual eBay item numbers are used this has been a nuisance for legitimate sellers.

### **3.4.5 False Escrow**

Another method is after winning a bid on items on the online auction site eBay (especially laptops or other consumer electronics), to suggest to use an escrow service. The escrow service is fraudulent and part of the scam. The victim will send the laptop or camera to the escrow service, never to hear from the scammer or escrow service again. The website of the escrow service will typically go offline after the victim has sent his goods. Some scammers send e-mails masquerading as official e-mails from PayPal to convince the victim that the escrow method is perfectly normal procedure; some of the e-mails contain spelling errors.

A variation of this scam is to adopt a more personal approach. The "buyer" bids for and wins the item on sale, only to then claim that it is actually to be a gift for a relative and asks for it to be sent direct there, even if the seller has specified that he or she will ship only within his or her own country. In order to facilitate the scam, the fraudulent buyer will often create a brand new legitimate eBay user account complete with a false address that is apparently in the seller's home country, but which will not pass any kind of real inspection as the scammer will often create errors with the spelling, geography or postal code formats. As with escrow scams, the eBay ID will disappear as soon as the victim has sent the goods, and the scammers tend to target inexperienced first time, private sellers.

### **3.4.6 Hitman**

An e-mail is sent to the victim's inbox, supposedly from a hitman who has been hired by a "close friend" of the recipient to kill him/her, but will call off the hit in exchange for a large sum of money. This is usually backed up with a warning not to contact the police, or the "hitman" will be forced to go through with the plan.

### **3.4.7 eBay/Western Union Scam**

This scam involves eBay and the appeal of high priced goods, usually electronics, for a bargain price. A seller will advertise an item (camera, laptop, plasma TV) at low cost. The body of the ad instructs buyers to contact the seller directly outside of eBay at a yahoo or hotmail type account. When contact is made, the seller gives a long story about his problems receiving payment by Paypal - eBay's payment arm. The seller insists that the buyer send money by Western Union. The allure is that the product is a huge bargain; (eg. \$2000 item for \$700) Of course, if money is sent, it is gone forever and no product is ever delivered. The phony seller usually has a list of prepared e-mails to respond quickly to questions from buyers; he'll go on about how his integrity is important, how he wouldn't risk his family's name, he's legit, check 'his' feedback, etc.

The phony seller makes the listing look credible by using a real eBay id to list the item. The real id has been stolen from a legitimate seller with good feedback, usually by means of e-mail phishing.

### **3.4.8 Lottery Scam**

Lottery scam involves fake notices of lottery wins. The winner will usually be asked to send sensitive information to a free e-mail account. This is a form of advance fee fraud as money in advance is often required and is also similar to phishing.

Much like the Auction overpayment fraud detailed above, a new variant of the lottery scam involves fake or stolen checks being sent to the "winner" of the lottery (these checks representing a part payment of the winnings). The winner will then be more likely to assume that the win is legitimate and subsequently more likely to send the fee (which he does not realise is an advance fee). The check, and associated funds, will then be flagged by the bank when the fraud is discovered and debited from the victim's account.

### **3.4.9 Inheritance Scam**

A variant of the scam will appear to be sent by a lawyer representing the estate of some long-lost relative the victim never knows he or she had (the victim's surname will be inserted into the e-mail message) who perished along with his or her family in a car or airplane accident a short period of time ago (usually a few months). The scammer will claim to have gone to a lot of trouble to find the victim in order to give him or her a share of the millions of dollars available if the victim will forward his or her bank account information to the scammer.



### **3.4.10 False Online Storefront Scam**

A website is set up offering too-good-to-be-true prices on popular goods. For an undisclosed reason payment cannot be made using credit cards or checks but only via untraceable means such as Western Union or e-gold. The buyer pays the money but never receives the goods, and is unable to reverse the transaction.

### **3.4.11 Classified Advertisement Scams**

In a classified advertisement scam, scammers respond to an advertisement for anything that is being advertised at a reasonably high price (for example a car, a computer or a snowboard). There are various variants of this scam; typically, scammers, after an initial phase of feigned interest, agree to buy the item and offer to pay for it with a cheque with a much higher value than the agreed price, using various excuses. The scammer will ask to have most of the difference paid back in cash at time of collection, supposedly leaving the rest to the victim as a reward for their flexibility and inconvenience. The collection will be arranged soon after the money will be made available in the victim's bank account. The victim will not realise that having the funds available is different from having the cheque cleared, and therefore will happily agree to the terms. The cheque clearing process can take weeks, after which the bank will claim the whole sum back because the cheque is fake.

This is also used over the IP Relay. There is a case where the scammer requests a driver's license or international passport be faxed over as he represents a close friend of his who is dying.

### **3.4.12 Tutor Scams**

In this variation the scammer responds to an ad placed by a tutor-for-hire, such as a music instructor, explaining his need for a tutor for his child who will soon be relocating to the tutor's area. Often the scammer will want a suspiciously high amount of instruction for his child and will of course want to pay for multiple weeks of instruction in advance via money order or cashier's check. The dead give-away is usually the scammer's request for very specific list of information e.g. "full name, address, city, state, phone number" in the first or second e-mail. The rest of the scam is the same as other fake check/wire transfer scams, where a fake check or money order for more than the agreed price is sent to the victim, then the scammer requests that the victim wire the balance back to him or someone he owes a debt.

### **3.4.13 Escort Scams**

In this variant of a classified advertisement scam, a scammer answers an online escort advertisement, typically posing as a wealthy businessman traveling from Nigeria or London to the escort's city of residence. The scammer contacts an escort claiming to be interested in a long-term companionship arrangement of days or even weeks in length, the total time involved totalling to a substantial sum of money. The scammer offers to pay in advance by cheque in excess of the net payment and asks for remittance of the balance. This version is especially popular as escorts in many cases cannot safely contact legal authorities for any reason and are unlikely to report successful or attempted fraud. A variant of the escort scam involves translators and interpreters who are asked to escort a businessman or his family for a few days.

#### **3.4.14 Black Money Scam**

Black money scam or *wash wash*: A "money cleaning" scam involving a huge amount of black papers (purportedly \$100 USD bank notes covered by a black film to sneak them past the custom officers) that is shown to the victim, who is then requested to pay for "expensive chemicals" to cleanse the bills.

#### **3.4.15 Rental Scams**

Where the victim (i.e., a prospective tenant) is seeking to rent accommodation, the scammer will answer a classified advertisement offering a high-standard place for low cost, even showing pictures of the said rooms. The victim is required to pay a deposit, but once the scammer has received the deposit he will disappear leaving the victim out-of-pocket.

Where the victim (e.g., landlord) is looking to find a tenant for their accommodation, the scammer poses as an "interested" party who is seeking to move to the said location. On inquiry to the prospective tenant, the victim receives a follow up e-mail indicating they will be sent a cheque by the tenant's new employer that will cover the rent, plus the new "tenant's" living expenses (e.g., to purchase furniture). The victim is asked to forward the additional portion to their new "tenant" by Western Union (or similar).

Where the victim posts on a communal website (e.g. Craigslist) that he/she is looking for a roommate to share a rental unit (or is a landlord looking to rent a unit), and the "scammer" poses as an interested party and sends a check to hold the room. The check will originate from overseas. The victim receives the check and deposits it into his /her bank account and that amount of money will temporarily appear as having

been added in. Within a few days the scammer then contacts the victim and advises that he/she cannot move into the rental unit due to an illness. The scammer will even provide documents indicating this state of ill health. The scammer then asks the victim to immediately wire transfer the money from the check back to him/her. This takes place, and then a few days later the victim finds out from his/her bank that the original check has bounced.

### **3.4.16 Puppy Scam**

Much like the other scams detailed here this involves the promise of an item when all the necessary fees have been advanced. Adverts are taken out by someone who is claiming they are the breeder of puppies they sold and that they are not doing well in their current situation. The owner claims to be looking for someone to adopt them back. They also claim to work as a missionary or for the United Nations. The advance fees in this case being for the purchase of the animal and *Customs* charges that will never end.

Calls are also made through instant IP Relay to unsuspecting callers. The callers will give the victim their e-mail address to e-mail them all details and final price of the puppy. E-mail content is unknown but due to the confidentiality of the Ip-Relay system operators cannot disconnect the calls. One theory is that the scammers scam and receive pure bred puppies, breed the puppies and sell them back to US buyers.

## **3.5 Consequences**

### **3.5.1 Monetary Loss Estimates**

Estimates of the total losses due to the scam vary widely. The Snopes website lists the following estimate.

“The scam is hugely successful.” According to a 1997 newspaper article “We have confirmed losses just in the United States of over \$100 million in the last 15 months,” said Special Agent James Caldwell, of the Secret Service financial crimes division. “And that's just the ones we know of. We figure a lot of people don't report them.”

Although the "success rate" of the scam is hard to gauge, some experienced 419 scammers get one or two interested replies for every thousand messages. It is claimed that an experienced scammer can expect to make several thousand dollars per month.

Ultrascan Advanced Global Investigations, a Netherlands-based firm which has been studying 419 matters since the mid-1990s, has prepared

a table quantifying 419 operations by country for 2005 and 2006. These stats are based on Ultrascan's in-house investigations and include, by nation: number of 419 rings; number of 419ers; income of the 419ers (the amount of losses by victims to the 419ers); and additional data. 419 Coalition view is that these stats present a reasonably conservative and realistic look at the extent and magnitude of 419 criminal operations worldwide.

Since 1995, the United States Secret Service has been involved in combating these schemes. The organisation will not investigate unless the monetary loss is in excess of fifty thousand US Dollars. However, very few arrests and prosecutions have been made due to the international aspect of this crime.

In 2006, a report by a research group concluded that scams cost the UK economy £150 million per year, with the average victim losing £31,000.

### **3.5.2 Physical Harm or Death**

Some victims have hired private investigators in the fraudster's country or have personally travelled to the fraudster's country, without ever retrieving their money. There are cases of victims being unable to cope with the losses and committing suicide.

In February 2003, a scam victim from the Czech Republic shot and killed the person who defrauded him.

Leslie Fountain, a senior technician at Anglia Polytechnic University in England, set himself on fire after falling victim to a scam; Fountain died of his injuries.

### **3.5.3 Kidnapping**

Kensuke Matsumoto, a Japanese national, fled his kidnappers in Durban, South Africa after falling victim to a 419 scheme in 1999.

Joseph Raca, a former mayor of Northampton, England, was kidnapped by scammers in Johannesburg, South Africa in July 2001. The captors released Raca after they became nervous.

Danut Tetrescu, a Romanian who flew from Bucharest to Johannesburg to meet with con men in the Soweto area of Johannesburg, was kidnapped in 1999 and held for \$500,000.

### **3.5.4 Murder**

29-year old George Makronalli, a Greek man, was murdered in South Africa after responding to a 419 scam.

Kjetil Moe, a Norwegian businessman, was reported missing and ultimately killed after a trade with a scammer in Johannesburg, South Africa (September 1999).

Mary Winkler is awaiting trial over the shooting of her pastor husband on March 22, 2006, after allegedly being taken for \$17,500 in a 419 scam.

One American was murdered in a country in June 1995 after being lured by a 419 scam.

### **3.5.5 Arrests**

In 2004, fifty-two suspects were arrested in Amsterdam after an extensive raid. An Internet service provider had noticed the increased email traffic. None was jailed or fined, due to lack of evidence. They were released in the week of July 12, 2004. An entirely phony "embassy" was also discovered in Amsterdam; another allegedly exists in Bangkok.

### **3.5.6 The Victim Becomes a Criminal**

Victims of the fraud often fall directly into crime by "borrowing" or stealing money to pay the advanced fees, thinking an early payday is imminent.

One example of this was Robert Andrew Street, a Melbourne based financial adviser, who fleeced his clients for over AU\$ 1,000,000 which he sent to the scammers in the hope of receiving USD\$65M in return. Eventually the Australian Securities and Investments Commission (ASIC) investigated the victim, who had now become a conman himself.

Another example was a bookkeeper for Michigan law firm Olsman Mueller & James who in 2002 emptied the company bank account of USD\$2.1M in expectation of a USD\$4.5M payout. John W. Worley fell for a scam and was convicted of taking money under false pretenses.

Mark Whitacre defrauded Archer Daniels Midland, a food products manufacturer for which he was a division president, embezzling \$9 million during the same period of time that he was acting as an informant for the FBI in a price-fixing scheme that ADM was involved in. His illegal activities in trying to procure funds for payment of his supposed benefactors cost him his immunity in the price-fixing scandal.

### **3.5.7 Impeded E-mail Output**

Legitimate businesses find that their e-mails increasingly fail to reach their targets, due to people and companies setting their e-mail clients to automatically mark all mail containing the words relating to a host country with high rate of fake and fraudulent e-mails or coming from that country's IP addresses as spam, or even delete it out of hand.

### **3.6 Proposed Legislation**

As a result of the fraud, countries are drafting legislation to make spamming a criminal offence punishable with a fine up to £2,000GBP and three years in jail.

## **4.0 CONCLUSION**

Advance fee fraud is totally unacceptable by reputable and accountable individuals, organisations and nations. These schemes are out to forestall the good work made possible by advances in technology, especially information and communications technologies. Organisations, agencies and nations are to collaborate to eradicate the menace of advance fee fraud, now.

## **5.0 SUMMARY**

- An advance fee fraud is a confidence trick in which the target is persuaded to advance relatively small sums of money in the hope of realising a much larger gain.
- The 419 scam originated in the early 1990s as the oil-based economy of Nigeria went downhill. Several unemployed university students first used this scam as a means of manipulating business visitors interested in shady deals in the Nigerian oil sector before targeting businessmen in the West, and later the wider population.
- The investors are contacted, typically with an offer of the type "A rich person from the needy country needs to discreetly move money abroad, would it be possible to use your account?"
- Some London-based gangs have been known to use spam ware on laptops which they surreptitiously connect to the cafe's network, but even this software is notably out-of-date.
- Sometimes, victims are invited to a country to meet real or fake government officials. Some victims who do travel are instead held for ransom.
- A recent variant is the "Romance Scam" which is a money-for-romance angle. The victim is usually approached on an online dating service and becomes interested in a "lady" or "man" who has

attractive pictures posted, generally stolen from online portfolios of modeling agencies

- A variation on the eBay scam involves sending a request for payment for an item that the alleged seller does not own but claims to have sent. Since actual eBay item numbers are used this has been a nuisance for legitimate sellers.
- Lottery scam involves fake notices of lottery wins. The winner will usually be asked to send sensitive information to a free email account.
- In a classified advertisement scam, scammers respond to an advertisement for anything that is being advertised at a reasonably high price (for example a car, a computer or a snowboard).
- In this variation the scammer responds to an ad placed by a tutor-for-hire, such as a music instructor, explaining his need for a tutor for his child who will soon be relocating to the tutor's area
- In this variant of a classified advertisement scam, a scammer answers an online escort advertisement, typically posing as a wealthy businessman traveling from a country or London to the escort's city of residence.
- Where the victim (e.g., landlord) is seeking to find a tenant for their accommodation, the scammer poses as an "interested" party who is seeking to move to said location.
- Much like the other scams detailed here this involves the promise of an item when all the necessary fees have been advanced. Adverts are taken out by someone who is claiming they are the breeder of puppies they sold and they are not doing well in their current situation.
- Although the "success rate" of the scam is hard to gauge, some experienced 419 scammers get one or two interested replies for every thousand messages. It is claimed that an experienced scammer can expect to make several thousand dollars per month.
- Legitimate businesses find that their e-mails increasingly fail to reach their targets, due to people and companies setting their e-mail clients to automatically mark all mail containing the words relating to a host country with high rate of fake and fraudulent e-mails or coming from that country's IP addresses as spam, or even delete it out of hand.

## **6.0 TUTOR-MARKED ASSIGNMENT**

1. Discuss five ways in which you can detect if an e-mail is fraudulent.
2. Mention five negative outcomes of advance fee fraud.

## **7.0 REFERENCES/FURTHER READINGS**

British Broadcasting Corporation. Suicide of Internet Scam Victim

Con artists target phone system for the deaf, MSNBC

Comptroller of the Currency Administrator of National Banks Alert  
2007-12

Dear Mick Jaeger. *Ravi Tek*.

FTC Consumer Alert

“Internet Technology Fueling Nigerian Scam.” *Journal of the American Veterinary Medical Association* (2003-04-01).

Mayer, Caroline E. "Banks Honor Bogus Checks and Scam Victims Pay", *The Washington Post*( 2006-06-01), p. A01.

*Nigerian Criminal Code*

*Snopes* (2003-09-06). Nigerian Scam.

Nigeria Scams “Cost UK Billions”. *BBC News* (20 November, 2006).

Philip de Braun. “SA Cops, Interpol Probe Murder”, Radio Prague, (2003-02-20), “*Czech pensioner charged with murdering Nigerian consul*”.

Scams that Keep Being Used on People

*The Register* (Tuesday 19th October 2004). “419ers Take Aussie Financial Advisor for AU\$1m”.

*The Guardian* (2005-10-15). “Woman Falls for Nigerian Scam, Steals \$2.1m from Law Firm”.

*The Guardian* (2005-10-15). “Spammers Face Jail Terms Under Proposed Law”.

## **MODULE 2**

Unit 1	Electronic Fraud (3) <i>Credit Card Fraud and Forex Scam</i>
Unit 2	Strategic Fraud Detection
Unit 3	Electronic Fraud Detection Techniques
Unit 4	Control and Auditing Of Information System
Unit 5	Guidelines For Electronic/Internet Banking Audit Programme



## **UNIT 1      ELECTRONIC FRAUD (3)    *CREDIT CARD FRAUD AND FOREX SCAM***

### **CONTENTS**

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
  - 3.1 Types of Credit Card Fraud
  - 3.2 Credit Card Crime Profits, Losses & Punishment
    - 3.2.1 Losses
    - 3.2.2 Credit Card Companies
    - 3.2.3 The Criminals
  - 3.3 Reporting Credit Card Fraud
  - 3.4 Forex Scam
    - 3.4.1 CFTC Warnings
    - 3.4.2 The Use of High Leverage
  - 3.5 Wire Fraud
  - 3.6 Developing an Information Management Policy
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

### **1.0 INTRODUCTION**

**Credit card fraud** is a kind of fraud where a merchant (business, service provider, seller, etc.) is “tricked” into releasing merchandise or rendering services, believing that a credit card account will provide payment for goods/services. The merchant later learns that they will not be paid, or the payment they received will be reclaimed by the card's issuing bank.

Typically, the fraudster causes a credit card of another person to be charged for a purchase. Today, half of all credit card fraud is conducted online, meaning that the fraudsters make online purchases with the credit card details of other people.

### **2.0 OBJECTIVES**

At the end of this unit, you should be able to:

- differentiate advance fee fraud from credit card and forex fraud
- define credit card fraud
- define forex fraud
- identify the different types of credit card and forex fraud

- explain the revenue profile of credit card companies
- highlight some agency warnings that concern forex business
- identify the essential elements of wire fraud.

### **3.0 MAIN CONTENT**

#### **3.1 Types of Credit Card Fraud**

##### **1. Stolen Card Fraud**

When a card holder loses or has their credit card stolen, it is possible for the thief to make unauthorised purchases on that card up until the card is cancelled. A thief can potentially purchase thousands of dollars in merchandise or services before the card holder and the bank realise that the card is in the wrong hands. Self-serve payment systems such as gas stations are also highly prone to accepting a stolen credit card, as there is no verification of the card holder's identity, however many stations are trying to prevent this by adding a check requiring the user to key in a zip code. The zip code must match the code registered to the credit card or the transfer will fail.

##### **2. Credit Card Mail Order Fraud**

Using a stolen credit card number, or computer generated card number, a thief will order stolen goods. This type of fraud is now known as “Card Not Present” (CNP) referring to card transactions that are requested by mail, telephone or over the Internet when the cardholder is not present at the point of sale. VISA points out that CNP must take extra precaution against fraud exposure and associated losses. Anonymous scam artists bet on the fact that many fraud prevention features do not apply in certain environments. 3-D Secure is an authentication protocol developed by Visa and MasterCard to protect online card payments, in which the card owner has to register with the issuing bank.

##### **3. Skimming**

Skimming is the theft of credit card information by a dishonest employee of a legitimate merchant, manually copying down numbers, or using a magnetic stripe reader on a pocket-sized electronic device. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The skimmer will typically use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip.

Many instances of skimming have been reported where the perpetrator has put a device over the card slot of a public cash machine (Automated Teller Machine), which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pinhole camera to read the user's PIN at the same time.

To prevent this type of fraud, cards in countries such as the UK are issued featuring a smart chip with public key encryption. The chip cannot be copied, but the card number, expiry date and security code can be, and this set of data is often sufficient to use the victim's credit card account for fraudulent purposes with so-called "card not present" transactions, e.g., manual input, over the telephone or Internet.

#### **4. Carding**

Carding is a term used by fraudsters for a process they use to verify that sets of stolen credit card data are still valid. The fraudster will present each set of credit card details in turn on a website that has real-time transaction processing, making a purchase for a very small monetary amount so as not to use up the card's credit limit, and so as not to attract the attention of a human reviewer to the transaction.

Often, an online donation site for a charity is used instead of an eCommerce merchant, since there is no need to find an item of a suitable price to put in the virtual shopping cart, nor to supply shipping details. The carder may do this manually with a web browser, or may write automated software to interface to the website's checkout or billing forms. Often, an online donation site for a charity is used instead of an eCommerce merchant, since there is no need to find an item of a suitable price to put in the virtual shopping cart, nor to supply shipping details. The carder may do this manually with a web browser, or may write automated software to interface to the website's checkout or billing forms.

In the past, carders used to use computer programs called "generators" to produce a sequence of credit card numbers, and then test them to see which valid accounts. However, this process is no longer viable due to widespread requirement by Internet credit card processing systems for additional data such as the billing address, the 3 to 4 digit Card Security Code and/or the card's expiry date. Nowadays, carding is more typically used to verify credit card data obtained directly from the victims by skimming or phishing.

A set of credit card details that has been verified in this way is known in fraud circles as a phish (see Phishing). A carder will typically sell data files of phish to other individuals who will carry out the actual fraud. Market price for a phish ranges from US\$1.00 to US\$50.00 depending on the type of card, freshness of the data and credit status of the victim.

## **3.2 Credit Card Crime Profits, Losses & Punishment**

### **3.2.1 Losses**

U.S. Federal Law can hold the cardholder victim responsible for up to \$50. Merchants in high-risk industries like unattended automated fuel pumps or Internet sales, anticipate a certain amount of credit card fraud, and set prices accordingly. These higher costs are then passed onto the customer.

### **3.2.2 Credit Card Companies**

In 2003 the *Wall Street Journal* estimated that the credit card industry generated \$500,000,000 in annual revenue in research and investigation fees paid by consumers and businesses. This additional revenue offsets some of the costs incurred by credit card issuing and processing companies when investigating chargeback claims. Since 2005, credit card fraud in the UK and America has increased by 350% on average (figures from Reuters). Some merchants believe the high revenue generation by the banks from the crime victims reduces the incentive for the credit card banks to implement procedures to reduce credit card crime. However, the companies which collect these fees are not capable of dictating fraud prevention policies to the rest of the world. Payment transfer associations, like Visa and MasterCard receive profit from transaction fees calculated as a percentage of the amount of money they transfer. These associations are motivated to enact policies which increase the amount of money transferred by their systems. Credit card fraud has a chilling effect on merchant acceptance of credit cards, motivating merchants not to accept credit card payments to mitigate their risk of loss. These payment transfer associations are therefore motivated to enact policies and enforce regulations which reduce credit card fraud.

Merchants have begun to request changes in state and federal laws to protect consumers and merchants from fraud, but the credit card industry has opposed many of the requested laws.

Because all card-accepting merchants and card-carrying customers are bound by contract law, according to the agreements they sign with their processing / issuing banks, respectively, state and federal law has a

smaller role in preventing merchants from being tricked. Payment transfer associations enact regulatory changes, and issuing / acquiring banks, merchants, and cardholders are contractually bound to these new regulations.

### 3.2.3 The Criminals

In the US, persons that commit credit card crimes largely go unpunished and repeatedly victimise consumers and businesses. The Secret Service handles crimes involving the US money supply; they have a limit of \$2,000 before investigating each crime. Most credit card criminals know this and keep purchases from any one business below \$2,000. With credit card crimes occurring across state lines, criminals often are never prosecuted because the dollar amounts are too low for local law enforcement to pay for extradition.

## 3.3 Reporting Credit Card Fraud

If you lose or have had your credit card stolen, you should immediately report it to your card issuer. Once you report the incident, you are no longer responsible for unauthorised charges made on your card.

In the US, credit card fraud can be reported to the Federal Trade Commission (FTC) and to local and regional authorities. It is the standing policy of the FTC not to investigate reports where the value of fraud does not exceed \$2000. Local law enforcement may or may not further investigate a credit card fraud, depending on the amount, type of fraud, and where the fraud originated from.

If you are a merchant and you suspect orders have been placed for your products/services using stolen credit card information you will need to contact VISA/MC/AMEX/DISCOVER to obtain the issuing bank's phone number then call the bank to report that you suspect that their customer's credit card information has been stolen.

## 3.4 Forex Scam

A **forex scam** is any trading scheme used to defraud individual traders by convincing them that they can expect to unreasonably profit by trading in the foreign exchange market, which would be a zero-sum game were it not for the fact that there are brokerage commissions, which technically make forex a “negative-sum” game.

These scams might include churning of customer accounts for the purpose of generating commissions, selling software that is supposed to

guide the customer to large profits,<sup>[1]</sup> improperly managed “managed accounts”, false advertising, Ponzi schemes and outright fraud. It also refers to any retail forex broker who indicates that trading foreign exchange is a low risk, high profit investment.

The U.S. Commodity Futures Trading Commission (CFTC), which loosely regulates the foreign exchange market in the United States, has noted an increase in the amount of unscrupulous activity in the non-bank foreign exchange industry.

An official of the National Futures Association was quoted as saying, “Retail forex trading has increased dramatically over the past few years. Unfortunately, the amount of forex fraud has also increased dramatically...” Between 2001 and 2006 the U.S. Commodity Futures Trading Commission has prosecuted more than 80 cases involving the defrauding of more than 23,000 customers who lost \$300 million, mostly in managed accounts. CNN also quoted Godfried De Vidts, President of the Financial Markets Association, a European body, as saying, “Banks have a duty to protect their customers and they should make sure customers understand what they are doing. Now if people go online, on non-bank portals, how is this control being done?”

The highly technical nature of retail forex industry, the OTC nature of the market, and the loose regulation of the market, leaves retail speculators vulnerable. Defrauded traders and regulatory authorities can find it very difficult to prove that market manipulation has occurred since there is no central currency market, but rather a number of more or less interconnected marketplaces provided by interbank market makers.

### **3.4.1 CFTC Warnings**

The CFTC lists nine warning signs for foreign exchange trading fraud:

#### **1. Stay away from Opportunities that seem too good to be true**

Always remember that there is no such thing as a "free lunch." Be especially cautious if you have acquired a large sum of cash recently and are looking for a safe investment vehicle. In particular, retirees with access to their retirement funds may be attractive targets for fraudulent

operators. Getting your money back once it is gone can be difficult or impossible.

## **2. Avoid any Company that Predicts or Guarantees Large Profits**

Be extremely wary of companies that guarantee profits, or that tout extremely high performance. In many cases, those claims are false.

- “Whether the market moves up or down, in the currency market you will make a profit.”
- “Make \$1000 per week, every week”
- “We are out-performing 90% of domestic investments.”
- “The main advantage of the forex markets is that there is no bear market.”
- “We guarantee you will make at least a 30-40% rate of return within two months.”

## **3. Stay away from Companies that Promise little or no Financial Risk**

Be suspicious of companies that downplay risks or state that written risk disclosure statements are routine formalities imposed by the government.

The currency futures and options markets are volatile and contain substantial risks for unsophisticated customers. The currency futures and options markets are not the place to put any funds that you cannot afford to lose. For example, retirement funds should not be used for currency trading. You can lose most or all of those funds very quickly trading foreign currency futures or options contracts.

Therefore, beware of companies that make the following types of statements:

- “With a \$10,000 deposit, the maximum you can lose is \$200 to \$250 per day.”
- “We promise to recover any losses you have.”
- “Your investment is secure.”

## **4. Don't Trade on “Margin” unless you understand what it Means**

Margin trading can make you responsible for losses that greatly exceed the dollar amount you deposited.

Many currency traders ask customers to give them money, which they sometimes refer to as "margin," often sums in the range of \$1,000 to \$5,000. However, those amounts, which are relatively small in the currency markets, actually control far larger dollar amounts of trading; a fact that often is poorly explained to customers.

Don't trade on margin unless you fully understand what you are doing and are prepared to accept losses that exceed the margin amounts you paid.

#### **5. Question Firms that Claim to Trade in the "Interbank Market"**

Be wary of firms that claim that you can or should trade in the "interbank market," or that they will do so on your behalf.

Unregulated, fraudulent currency trading firms often tell retail customers that their funds are traded in the "interbank market," where good prices can be obtained. Firms that trade currencies in the interbank market, however, are most likely to be banks, investment banks and large corporations, since the term "interbank market" refers simply to a loose network of currency transactions negotiated between financial institutions and other large companies.

#### **6. Be Wary of Sending or Transferring Cash on the Internet, by Mail or Otherwise**

Be especially alert to the dangers of trading online; it is very easy to transfer funds online, but often can be impossible to get a refund.

It costs an Internet advertiser just pennies per day to reach a potential audience of millions of persons, and phony currency trading firms have seized upon the Internet as an inexpensive and effective way of reaching a large pool of potential customers.

Many companies offering currency trading online, are not located within the United States and may not display an address or any other information identifying their nationality on their website. Be aware that if you transfer funds to those foreign firms, it may be very difficult or impossible to recover your funds.

#### **7. Currency Scams Often Target Members of Ethnic Minorities**

Some currency trading scams target potential customers in ethnic communities, particularly persons in the Russian, Chinese and Indian immigrant communities, through advertisements in ethnic newspapers



and television “infomercials.” Sometimes those advertisements offer so-called “job opportunities” for “account executives” to trade foreign currencies. Be aware that “account executives” that are hired might be expected to use their own money for currency trading, as well as to recruit their family and friends to do likewise. What appears to be a promising job opportunity often is another way many of these companies lure customers into parting with their cash.

## **8. Be Sure You Get the Company's Performance Track Record**

Get as much information as possible about the firm's or individual's performance record on behalf of other clients. You should be aware, however, that It may be difficult or impossible to do so, or to verify the information you receive. While firms and individuals are not required to provide this information, you should be wary of any person who is not willing to do so or who provides you with incomplete information. However, keep in mind, even if you do receive a glossy brochure or sophisticated-looking charts, that the information they contain might be false.

## **9. Don't Deal with anyone Who Won't Give You Their Background**

Plan to do a lot of checking of any information you receive to be sure that the company is and does exactly what it says.

Get the background of the persons running or promoting the company, if possible. Do not rely solely on oral statements or promises from the firm's employees. Ask for all information in written form. If you cannot satisfy yourself that the persons with whom you are dealing are completely legitimate and above-board, the wisest course of action is to avoid trading foreign currencies through those companies.

### **3.4.2 The Use of High Leverage**

By offering high leverage, the market maker encourages traders to trade extremely large positions. This increases the trading volume cleared by the market maker and increases his profits, but increases the risk that the trader will receive a margin call. While professional currency dealers (banks, hedge funds) never use more than 10:1 leverage, retail clients are generally offered leverage between 50:1 and 200:1, and even up to 400:1.

## **3.5 Wire Fraud**

**Wire fraud** is a legal concept in the United States Code which provides for enhanced penalty of any criminally fraudulent activity if it is determined that the activity involved electronic communications of any sort, at any phase of the event. As in the case of mail fraud, this statute is often used as a basis for a separate federal prosecution of what would otherwise have been only a violation of a state law.

For example, the crime of wire fraud is codified at 18 U.S.C. § 1343, and reads as follows:

- Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both. If the violation affects a financial institution, such person shall be fined not more than \$1,000,000 or imprisoned not more than 30 years, or both.

In one important case (*United States v. LaMacchia* -- text at [eff.org](http://eff.org)), an MIT student was charged with wire fraud when he could not be charged with criminal copyright infringement (having not personally profited from the online distribution of millions of dollars worth of illegally copied software). The United States District Court, District of Massachusetts, dismissed the charges, noting they were an attempt to find a broad federal crime where the more narrowly defined one had not occurred. Congress promptly amended the copyright law to limit further use of this loophole.

The alleged misrepresentation to support a conviction under 18 U.S.C. § 1343 must be a material misrepresentation. *Neder v. United States*, 527 U.S. 1, 23 (1999). A misrepresentation that is capable of influencing or has a “natural tendency” of influencing a decision is material. *Id.* at 13.

Thus, the essential elements of the crime of wire fraud are thus:

- (1) devise or intend to devise a scheme or artifice to defraud another person based on a material representation;
- (2) with the intent to defraud;
- (3) through the use of interstate wire facilities (e.g. telecommunications of any kind).
- (4) a fourth element will be included where the alleged victim is a financial institution, to enhance sentencing as provided in the statute.

#### 4.0 CONCLUSION

Just like the advance fee fraud, credit card, forex and wire frauds wreck economies and organisations and therefore should be fought by all concerned agencies. It is noteworthy that several counter measures have been developed to thwart the efforts of the perpetrators of these fraud schemes. These fraudulent schemes prevent genuine businesses in forex trade and in the use of credit cards to ease financial transactions.

These schemes are out to forestall the good work made possible by advances in technology, especially information and communications technologies.

## 5.0 SUMMARY

- **Credit card fraud** is a kind of fraud where a merchant (business, service provider, seller, etc.) is “tricked” into releasing merchandise or rendering services, believing that a credit card account will provide payment for goods/services.
- When a cardholder loses or has their credit card stolen, it is possible for the thief to make unauthorised purchases on that card up until the card is cancelled.
- Skimming is the theft of credit card information by a dishonest employee of a legitimate merchant, manually copying down numbers, or using a magnetic stripe reader on a pocket-sized electronic device.
- Carding is a term used by fraudsters for a process they use to verify that sets of stolen credit card data are still valid.
- U.S. Federal Law can hold the cardholder victim responsible for up to \$50. Merchants in high-risk industries, like unattended automated fuel pumps or Internet sales, anticipate a certain amount of credit card fraud, and set prices accordingly.
- If you lose or have had your credit card stolen, you should immediately report it to your card issuer. Once you report the incident, you are no longer responsible for unauthorised charges made on your card.
- A **forex scam** is any trading scheme used to defraud individual traders by convincing them that they can expect to unreasonably profit by trading in the foreign exchange market, which would be a zero-sum game.
- An official of the National Futures Association was quoted as saying, “Retail forex trading has increased dramatically over the past few years. Unfortunately, the amount of forex fraud has also increased dramatically”.
- Many currency traders ask customers to give them money, which they sometimes refer to as “margin,” often sums in the range of \$1,000 to \$5,000.

- Unregulated, fraudulent currency trading firms often tell retail customers that their funds are traded in the “interbank market,” where good prices can be obtained.
- Some currency trading scams target potential customers in ethnic communities, particularly persons in the Russian, Chinese and Indian immigrant communities, through advertisements in ethnic newspapers and television “infomercials.”
- Wire fraud is a legal concept in the United States Code which provides for enhanced penalty of any criminally fraudulent activity if it is determined that the activity involved electronic communications of any sort, at any phase of the event.
- In one important case (United States v. LaMacchia -- text at eff.org), an MIT student was charged with wire fraud when he could not be charged with criminal copyright infringement (having not personally profited from the online distribution of millions of dollars worth of illegally copied software).

## **6.0 TUTOR-MARKED ASSIGNMENT**

1. Identify and define types of credit card frauds.
2. Discuss briefly the warnings signals by Commodity Futures Trading Commission to avoid Foreign Exchange fraud

## **7.0 REFERENCES AND FOR FURTHER READINGS**

CFTC News Release 4789-03, May 21, 2003. “SOFTWARE VENDOR CHARGED”.

CFTC Complaint Forex Advisory Firm and Trade Risk Management Firm Charged With Fraud.

Commodity Futures Trading Commission (CFTC) Release: 4946-0, “Fraud Charges Against Multiple Forex Firms”.

Foreign Currency Fraud Action, Commodity Futures Trading Commission (CFTC) vs. Donald O’Neill.

FOREX Advisory Commodity Futures Trading Commission's FOREIGN CURRENCY TRADING FRAUDS.

Forex Information, Commodity Futures Trading Commission (CFTC) Forex Information for Investors.

National Futures Association (NFA), NFA Launches Learning Programme.

## **UNIT 2      STRATEGIC FRAUD DETECTION**

### **CONTENTS**

- 1.0    Introduction
- 2.0    Objectives
- 3.0    Main Content
  - 3.1    A Case of Known Fraud
  - 3.2    Researches in the Use of Electronic Technology in Fraud Detection
  - 3.3    Fraud Fighting Activities
  - 3.4    Proactive Fraud Detection
  - 3.5    The Strategic Method of Fraud Detection
  - 3.6    Steps in Strategic Fraud Detection
    - 3.6.1   Understand the Business (Step1)

- 3.6.2 Identify Possible Frauds That Could Exist (Step 2)
- 3.6.3 Catalog Possible Fraud Symptoms for Each Type of Fraud (Step 3)
- 3.6.4 Use Technology to Gather Data about Symptoms (Step 4)
- 3.6.5 Analyse and Refine Results (Step 5)
- 3.6.6 Investigate Symptoms (Step 6)
- 3.6.7 Follow Up and Iterate the Cycle (Optional Step 7)
- 3.6.8 Automate Detection Procedures (Optional Step 8)
- 3.7 Using Technology to Gather Data about Symptoms
- 3.8 Analyse and Refine Results
- 3.9 Symptoms of Known Fraud Case
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

## 1.0 INTRODUCTION

Fraud detection is becoming increasingly important to managers of organisations, to internal and external auditors, and to regulators. Recent events, such as revelations of fraud-related problems at HEALTHSOUTH, Enron, and WorldCom, and the Sarbanes-Oxley Act stress the importance of early detection of fraud. Financial statement frauds have weakened investor confidence in corporate financial statements, led to a decrease in market capitalisation, and have contributed to four of the 10 largest bankruptcies in history<sup>3</sup>.

Because a \$1 fraud against an organisation reduces net income by \$1 and because organisations usually have profit margins (net income / revenues) of 10 to 20 percent, additional revenue of 5 to 10 times the amount of the fraud must usually be generated to restore net income to its pre- fraud level. For example, a major automobile manufacturing company had a \$436 million fraud a few years ago. At the time, the company's profit margin was just under 10 percent, meaning that additional revenues of approximately \$4.36 billion had to be generated to bring net income to what it would have been without the fraud. Assuming automobiles sell for an average price of \$20,000 each, the company had to make and sell 218,000 additional automobiles to restore net income to its pre- fraud amount. If this fraud had been proactively detected earlier, the fraud loss would have been much smaller and the effect on the firm much less severe. It is because frauds are so costly that statement on Auditing Standards No. 99 (AICPA 2002)—recently issued by the American Institute of Certified Fraud Examiners—requires auditors to assess the risk of material misstatement in financial statements due to fraud.

## **2.0OBJECTIVES**

At the end of this unit, you should be able to:

- mention some known cases of electronic frauds
- identify ways to eliminate electronic fraud
- identify the categories of fraud fighting activities
- identify the steps in strategic fraud detection
- identify the symptoms of fraud cases.

The purpose of this unit is to formalise a strategic, technology -based fraud detection model and explore its elements. We begin by discussing why proactive fraud detection is so important. Next, we present the formalised model. Key technology issues are identified and discussed, including data extraction and warehousing, data analysis for fraud detection, and investigation. We conclude by summarising briefly a proactive application of this model to detect unknown fraud.

## **3.0MAIN CONTENT**

### **3.1A Case of Known Fraud**

Several years ago, a senior vice president of a bank embezzled nearly \$14 million over a 16-year period. When the fraud was discovered through a customer complaint, the bank sued its external auditors for negligence in not detecting the fraud. The fraud had been committed by manipulating, looting and abusing customer accounts and maintaining several slush accounts with sufficient funds to handle problems when customers complained.

To determine whose responsibility it was to detect the fraud, a strategic approach was used. For this fraud, the various kinds of symptoms that could have been present were identified and catalogued. Once the possible symptoms were known, 16 years of bank records (from microfiche and corporate databases) were combined into a searchable database. Using the searchable database, queries for possible symptoms previously identified were made. The actual symptoms that were found are listed in Appendix A.

All of the listed symptoms pointed to one member of management---the guilty senior vice president---as the perpetrator. With this case, it was already known that a fraud had been committed. The search of bank records for fraud symptoms was for the purpose of determining who should have detected the fraud. Using technology to find symptoms revealed evidence so strong that there remained little doubt that a fraud

had been committed, who the perpetrator was and who should have detected the fraud.

This case indicates that appropriate use of technology can provide help in analysing fraud that has already occurred. The important question, however, is whether a similar, technology -based, statistical approach can be used to detect fraud against organisations that hasn't yet been discovered and where no knowledge or suspicion (predication) that fraud is being committed exists.

### **3.2 Researches in the Use of Electronic Technology in Fraud Detection**

A search of the academic literature found few studies describing the use of technology to proactively detect fraud or the articulation of a model describing proactive, technology -based fraud detection. In 2000, Nieschwietz, et al., published a comprehensive literature review of empirical fraud -related audit research. This paper cites 35 empirical studies on fraud detection in the audit, accounting, and general business literature. It places the studies into the following four groups:

- 8 studies on fraud predictors (effectiveness of red flags in predicting fraud)
- 11 studies on unaided fraud risk assessments (how well auditors assess audit risk associated with fraud)
- 6 studies on mechanically-aided fraud risk assessments (how well auditors assess audit risk associated with fraud when aided by checklists, expert systems, or other means)
- 10 studies on audit plans and fraud detection (how audit plans are modified—or not modified—due to increased risk of fraud)

The review article cited no studies on technology -assisted analysis of data to find financial statement or internal fraud. A search of the literature since 2000 reveals a similar focus in current research (Knapp and Knapp 2001; Shelton, et al. 2001; Albrecht, et. al 2001a). Despite the lack of empirical work conducted to detect fraud using technology, some limited work has been done. This work is described in the following paragraphs.

Several decades ago, Deloitte and Touche conducted internal research into the use of statistical methods to focus on abnormal data. This research culminated into a product, Statistical Techniques for Analytical Review (STAR), which identified significant fluxuations in data that warranted further information. The STAR research has since been integrated into AuditSystem/2.



Blocher and Willingham (1988) published a chapter on using computers to conduct analytical procedures. Their research was general to audit techniques and not specific to fraud detection. However, they included a section on using regression modeling for trending and analysis of data.

More recently, information on Benford's Law and Digital Analysis has surfaced in the literature. Albrecht, et al. (2001b) discussed using digital analysis to locate companies billing fraudulent invoice amounts to other organizations. Nigrini (1999) discusses the use of digital analysis in accounts payable data, estimations in the general ledger, inventories, payments, and refunds. In addition, Nigrini gives a general history of Benford's Law. Hill (1996) describes Benford's Law and makes reference to Nigrini's use of digital analysis for accounting in his Ph.D. thesis.

Finally, Albrecht, *et al.* (2001b) described a case study where technology was used to find fraud in a major oil refinery. While several frauds were found, the paper stopped short of proposing a model for the use of technology. In addition, the study targeted fraud within an organisation rather than within financial statements.

Despite the initial interest in technology -based fraud - detection techniques, little work has been done (other than digital analysis) in recent literature. The wide availability of online and corporate data and the increasing limits of modern computers suggest it may be time to revisit fraud detection techniques from a technological perspective.

Auditors are concerned about assessing fraud risk accurately because of the high cost associated with too much or too little investigation. Doing too much investigation when fraud is not present adds little economic value; failure to investigate sufficiently when fraud is present usually results in significant or even catastrophic costs (Palmrose 1987; Nieschwietz, et al. 2000). The previous statement includes the hidden assumption that fraud investigation is expensive. If, with the use of technology and simple, definable models, this cost can be driven down, auditors may be able to incorporate fraud detection into routine audit procedures without adding significant costs.

### 3.3 Fraud Fighting Activities

Fraud -fighting activities can be grouped into three primary categories: prevention, detection, and investigation.

**Fraud prevention** includes such activities as designing corporate fraud policies, creating internal audit departments, implementing internal controls, whistle-blower systems, and publicising fraud occurrences.

Investigation involves steps taken to answer the questions of who, how, when, and why once fraud is suspected or “fraud predication” is present. Fraud detection includes both proactive and reactive activities targeted at finding the first indication that fraud might be occurring or undertaken to develop a “predication of fraud”. Most traditional fraud detection methods are reactive in nature---that is, they are initiated by tips or complaints, control overrides, or other indicators that someone observes or hears.

Proactive fraud detection involves aggressively targeting specific types of fraud and searching for their indicators, symptoms, or red flags. Early fraud detection is critical because the sizes of most frauds increase geometrically over time as perpetrators gain confidence that their schemes are not being detected.<sup>8</sup>

### **3.4 Proactive Fraud Detection**

Fraud detection can be categorised into technology -base and non-technology -based methods. We further categorise technology -related methods into the following two categories:

- (1) **Computerised** traditional methods, and
- (2) **Strategic methods.**

Strategic methods can be subdivided into those that focus on people, and focus on transactions and reports.

Focusing on people includes methods such as using artificial intelligence techniques and fuzzy logic to score personnel profiles or matching individuals against known “bad guy” lists. Focusing on transactions involves searching records and databases for fraud symptoms relating to sales, purchasing, payment, receipt, borrowing, or other types of transactions. Today's widespread use of relational and other databases to store transactions creates new opportunities to proactively search for fraud in businesses. In previous years, fraud audit techniques such as discovery sampling have been computerised to increase their efficiency. However, just as the computerisation of traditional corporate processes at the dawn of the computer age did little to make those processes more effective (Hammer 1990), traditional fraud detection methods require a “business process re-engineering” effort to fully utilise the power of modern computers and the large, rich data stores available to researchers.

### **3.5 The Strategic Method of Fraud Detection**

Traditional fraud detection typically begins with an indication or anomaly that something isn't right, such as anonymous tips, unusual financial statement relationships, or control overrides. These indicators, often called red flags, provide predication that fraud may exist. Management, auditors or fraud examiners investigate these indicators with additional research, computer queries, or interviews to determine whether red flags represent real fraud or are being caused by other factors. This approach can be viewed as an inductive method: it begins with anomalies brought to someone's attention and continues by researching additional events and data until it is determined that fraud may be causing the indicators. It is followed by investigations to determine what the actual nature of the anomalies is.

As was illustrated in the known bank fraud example at the beginning of the unit, and as was validated using the fraud detection case described briefly at the end of this paper, current technology and widespread use of electronic databases to record transactions have made it possible to reverse traditional methods--starting with specific fraud types and moving forward to determine whether indicators or red flags of those specific frauds exist. It is now possible to specifically target different types of frauds, analyse entire populations, and zero in on fraud before traditional indicators become egregious enough to be observed. This method is called the strategic method of fraud detection. This method is a proactive approach that targets industry- and company-specific fraud anomalies and patterns and mines data for indicators of specific fraud types.

### **3.6 Steps in Strategic Fraud Detection**

#### **3.6.1 Understand the Business (Step 1)**

In traditional, inductive fraud detection, fraud examiners typically do not have any specific fraud in mind; rather, they see or learn of an event or anomaly that provides predication and prompts investigation. Quite differently, the strategic process starts with an understanding of the business or unit being examined. Since each business environment is different--even within the same industry or firm-- fraud detection is largely an analytical process. The same fraud detection procedures cannot be applied generically to all businesses or even to different units of the same organisation. Rather than rely upon generic fraud detection methods or generic queries, examiners must gain intimate knowledge of

each specific organisation and its processes. Having a detailed understanding underlies the entire strategic fraud detection process. Understanding processes in an organisation or unit is similar to the activities undertaken when performing business process reengineering. Appendix B identifies some of the common methods used to understand business processes (Pressman 1997).

### **3.6.2 Identify Possible Frauds That Could Exist (Step 2)**

Once fraud examiners feel confident that they understand the business, they must determine what possible frauds might exist or could occur in the operation being examined. This risk assessment step requires an understanding of the nature of different frauds, how they occur, and what symptoms they exhibit. The fraud identification process begins by conceptually dividing the business unit into its individual functions. Most businesses or even subunits are simply too large and diverse for examiners to consider simultaneously. Dividing the business into its individual functions helps focus the detection process. For example, examiners might decide to focus directly on the manufacturing plant, the collections department, or the purchasing function.

In this step, people involved in the business functions are interviewed. Fraud examiners ask questions such as: Who are the players? What types of employees, vendors, or contractors are involved? How do insiders and outsiders interact with each another? What types of fraud could be committed against the company or on behalf of the company? How could employees or management acting alone commit fraud? How could vendors or customers acting alone commit fraud? How could vendors or customers working in collusion with employees commit fraud? During this stage, the fraud detection team should brainstorm potential frauds by type and player. The likely occurrence of the various frauds should be considered, and a laundry list of frauds that will be considered is developed.

### **3.6.3 Catalog Possible Fraud Symptoms for Each Type of Fraud (Step 3)**

Fraud is a crime that is rarely seen. Rather, only fraud symptoms are observed. Unfortunately, what often appears to be a fraud symptom ends up being explained by other, non- fraud factors. For example, a company's accounts receivable balance may be increasing at a rate that appears unrealistically high. While this increase could be the result of fraud, the increasing receivables balance could be the result of major customers having financial difficulties or a change in credit terms.

This step of the strategic approach involves carefully considering whether variations of the six types of symptoms could be present in the cataloged frauds identified in Step 2. A matrix, tree diagram, or brainstorming map can be created that correlates specific symptoms with specific possible frauds. For example, kickbacks from vendors to buyers might be characterised.

### **3.6.4 Use Technology to Gather Data about Symptoms (Step 4)**

Once symptoms are defined and correlated with specific frauds, supporting data are extracted from corporate databases and other sources. While we focus our discussion of this step on relational databases (because of their popularity) data can be similarly extracted from most types of data stores.

While traditional fraud -search procedures have prescribed sampling of data, technology -based fraud - detection queries should be run against full transaction populations. Any summarisation or sampling that is done to the data before the queries are executed limits the power of the detection process. Because even significant frauds can occur in very few transactions, the use of sampling potentially misses fraudulent records (sampling error) and circumvents the ability of computers to quickly analyse full populations.

In conducting this step, fraud examiners should be prepared for bureaucracies and rules that make it difficult to gain direct access to databases. Limiting direct data access to users is well intentioned and critical in organisations. Such limits prevent users from corrupting data or viewing information they should not have access to. However, fraud examiners using the strategic detection approach need to access and analyse all information in a given system. Permission and support of upper management in gaining access is very important for successful detection efforts. Fraud teams should consider including a member of the IT staff who already understands the system and can provide access. To effectively design and implement symptom queries, a technology expert should be part of the fraud detection team. This person must be skilled in two areas: database programming and fraud principles. Skill in database programming is this person's primary reason for being included on the detection team. He or she must access databases and understand relationships between data. This access requires an understanding of relational theory, mainframe and/or UNIX operating systems, and scripting languages. In addition, this person must have some understanding of fraud principles to effectively contribute to the fraud detection team. Technology experts may identify new fraud symptoms as they extract and analyse data from previous queries.

Because of the large size of typical organisational data stores, many queries are actually composed of several extractions combined with algorithms programmed in scripting languages. The technology expert should understand at least one scripting language, such as Visual Basic, Perl, Python, or PowerBuilder, to automate repetitive tasks on transaction sets.

### **3.6.5 Analyse and Refine Results (Step 5)**

Once relevant data are retrieved, they should be compared against expectations and models. Since very large data sets--normally composed of thousands of smaller subsets--are often analysed, computer programs should be written to perform automated analyses. These algorithms examine records and highlight anomalies, unknown values, suggestive trends, or outliers that can then be analysed directly by examiners.

While specific analyses are unique to the business being examined and the type of fraud being searched for, most searches include time series models. This is because fraud is often discovered by examining changes over time. Historical patterns within the data, rather than outside factors, often set the standard that data are measured against. Sharp and unexpected increases in spending, purchases, or labour often signal possible fraud.

Some analyses will prescribe an expected data distribution. For example, a company might have a policy of no overtime---meaning that an employee working 60 hours per week for several consecutive weeks should be investigated. More commonly, however, a company's historical trends in the data set the norm. Rather than research these trends manually, algorithms should be written to automatically calculate the averages or expected patterns. Generated norms often provide more consistent and reliable measures than norms established through other means. In effect, generated norms allow the data to “speak for themselves”.

While traditional mechanisms of gathering and analysing data are often cost prohibitive, the effective use of technology will mitigate this problem. The authors are currently creating an open-source, data extraction and analysis package called *Picalo*<sup>9</sup> that will automate common tests for fraud. Picalo goes beyond traditional audit software (such as ACL and IDEA) by focusing specifically on fraud -related analyses. Future work will test whether applications such as Picalo can dramatically decrease detection cost while maintaining detection success. In addition, Picalo will provide a means for research into efficient and effective methods and patterns of fraud detection to be encapsulated, tested, and refined.

### **3.6.6 Investigate Symptoms (Step 6)**

Once anomalies are highlighted and determined to be indicators of fraud, they are investigated either using traditional or technology-based approaches. Investigation of leads should only be done on anomalies that cannot be explained through continued analysis.

Many times traditional investigation into symptoms provides new insights that allow further refinement of algorithms and queries. Information about one anomaly often clears up other highlighted results. These serve to “purify” the computer-based methods and provide increasingly meaningful results.

### **3.6.7 Follow Up and Iterate the Cycle (Optional Step 7)**

Fraud examiners should follow up on all identified symptoms. While finding fraud is certainly the primary objective of follow up efforts, the process often highlights control weaknesses, ineffective systems, undocumented policies, and data errors. Each of these anomalies can be corrected to make company processes more efficient and effective. Follow-up not only involves eliminating control weaknesses and fixing system, but also involves dealing with perpetrators in ways that discourage future fraudulent acts (Albrecht 2003).

The fraud detection process described thus far provides valuable information that helps investigators, auditors, and managers better understand a business and the types of frauds that could be occurring. After the cycle has been completed, the detection team should review what has been learned and determine how it can be improved. With greater understanding, new tools, and a set of tested algorithms, the strategic fraud detection process can be started again. Iteration through the process should be more efficient and more effective than prior ones. The end result is a mature, tested process for detecting fraud and other anomalies.

### **3.6.8 Automate Detection Procedures (Optional Step 8)**

Since much of the detection process is computerised, subsequent iterations are normally faster because analyses, algorithms, and models are already programmed. As analyses become more and more refined, they can be integrated directly into business processes. They can be programmed into new systems to stop problems at the time of data entry or transaction. They can be used to prevent anomalies before they occur.

In addition, detective measures can be run at specified periods automatically. They can be run against databases during off-peak hours to minimise their effect on corporate systems. Procedures can be programmed to highlight errors and send results to security personnel. For example, each week a different analysis could be run during the weekend and e-mailed to a corporate security team member for review on Monday morning.

### **3.7 Using Technology to Gather Data about Symptoms**

While the team was completing the first phases of the strategic method, it concurrently worked to achieve direct access to the refinery's databases. Because of the sensitivity of these databases, the programmer was only able to gain access after convincing high-level executives why direct access was critically important. Once connected, the database programmer learned the data schema and determined the types of queries that could be run.

The team used several platforms to run queries, including Java, PowerBuilder, Paradox, and Perl. A time engine was constructed to iteratively run time-based queries that often took several hours to complete. Results were normally stored in ad-hoc data warehouses created from middle-level database platforms such as Paradox or MySQL. These results were often compilations of data pulled from various corporate servers. Determining actual queries to run to search for red flags involved extensive discussions with firm personnel, successive iterations, sensitivity analysis, and development of occasional heuristics to approximate suspected frauds.

### **3.8 Analyse and Refine Results**

Once the data for a given search were stored in an appropriate warehouse, the team analysed data subsets for specified patterns. Normally, expected patterns (such as average price for specific products) were generated directly from the data rather than from outside sources. Subsets were compared with these averages for anomalies. Some queries highlighted transactions that were beyond two or three standard deviations from the norm. Other queries looked for changes in costs over time (after the x-axis had been standardised across time).

Counts for the number of anomalies found for each contractor, work team, corporate buyer, or corporate approver were calculated for each



subset. Sorting transactions by counts provided insight into potential problems and possible frauds. When queries produced too many red flags to allow effective investigation, queries were refined and intervals were tightened to produce more egregious results. In some cases statistical models, such as multiple regression and time series analysis, were used to combine data from different systems and compute expectations and norms.

When the analysis was complete (after numerous iterations and refinements), 26 possible frauds were identified. For each of these frauds, corporate security and internal audit were told where to look, which days and employees or contractors to focus on, what the nature of the suspected fraud was, and the types of symptoms found. Corporate security and internal audit then investigated the laser-like evidence to see if actual fraud was being committed or whether the “symptoms” were being caused by other factors. As they pursued the symptoms, they often found control weaknesses and data errors that, while not representing actual fraud, needed to be improved and corrected. Other symptoms produced legitimate, non-fraud explanations. Most, however, represented actual fraud that was costing the company tremendous amounts of money, over \$1 million in one case. When one “fraudulent” contractor was notified about the “possible fraud,” it immediately wrote the company a check for several hundred thousand dollars.

### **3.9 Symptoms of Known Fraud Case**

The following symptoms were found in the known fraud case:

1. Exception reports, reflecting fraudulent transactions that exhibited unusual, atypical and otherwise questionable patterns of supervisor overrides, transactions with no apparent business purpose, and transactions involving unusually large amounts. This symptom came from internally used bank records and occurred at least 221 times.
2. Journal vouchers containing only one signature or incorrect information and/or reflecting transfers between different customers' accounts. This symptom was found on internally used bank records and occurred at least 22 times.
3. Deposit slips completed by the fraud perpetrator with missing information, incomplete customer names or where the name of the depositor did not match the name on the passbook and/or the account name in the bank's records. This symptom was found on internally used bank records and occurred at least 56 times.

4. Deposits and withdrawals exceeding \$5,000 in the perpetrator's passbook account. This symptom was found on internally used bank records and occurred at last 90 times.
5. Withdrawal vouchers completed by the fraud perpetrator, missing customer names or signatures and/or containing incomplete or inaccurate information. This symptom was found on internally used bank records and occurred at least 35 times.
6. Bank checks reflecting transfers between different customers' accounts or checks with altered dates. This symptom was found on internally used bank records and occurred at least 22 times.
7. Withdrawal vouchers and checks containing purported customer signatures by the fraud perpetrator readily distinguishable upon comparison from the customer's signature. This symptom was found on internally used bank records and occurred at least 73 times.
8. Withdrawal vouchers completed by the perpetrator showing a different name from the account name. This symptom occurred on internally used bank records and occurred at least 60 times.
9. Large negative available balances in slush and other customer accounts. This symptom was found on internally used bank records and occurred at least 15 times.
10. Split deposits of customer funds between accounts of different customers and/or deposits of customer checks where the fraud perpetrator received cash back. This symptom was found on internally used bank records and occurred at least 9 times.
11. CDs closed prematurely with proceeds placed in lower interest-bearing passbook accounts, sometimes with large penalties. This symptom was found on internally used bank records and occurred at least 42 times.
12. Customers not being present when accounts were opened and closed or when transactions were affected in the account. This symptom occurred on internally used bank records and occurred numerous times in 26 different slush accounts.
13. Large withdrawals of cash by the fraud perpetrator from customer accounts. This symptom was found on internally used bank records and occurred at least 221 times.

14. The mailing of customer account statements to the fraud perpetrator's home instead of to the customer, without written authorisation. This symptom was found on internally used bank records and occurred in at least 40 different accounts.

## **4.0 CONCLUSION**

The strategic method of fraud detection is an effective way to detect and describe both known and unknown frauds. When used proactively to detect unknown fraud, it provides laser-like accuracy that allows for much more efficient investigation than the traditional shotgun approaches that have been used in the past. Disadvantages of the strategic method are (1) that it is more expensive to implement than reactive and inductive fraud detection methods and (2) it requires significantly more effort and expertise from team members. With repeated applications, however, economies of scale can be gained and fraud detection approaches can be automated. It is most suited to entities that have large, digital data stores and the ability to support this larger effort.

In this unit, the strategic approach was used to detect fraud against organisations---one by a bank vice president and another by contractors against an oil refinery. In the future, we will determine whether this deductive approach can be used to detect financial statement fraud.

This strategic method of fraud detection provides new power to fraud examiners that traditional methods cannot provide. It is a custom-tailored, full-population analysis directed at specific types of fraud. Using this method, fraud examiners and managements do not have to wait for "chance" indications or red flags of fraud to appear before investigative action is taken. The strategic method allows proactive detection of fraud before significant damage is done.

## **5.0 SUMMARY**

- Fraud detection is becoming increasingly important to managers of organisations, to internal and external auditors, and to regulators.
- A search of the academic literature found few studies describing the use of technology to proactively detect fraud or the articulation of a model describing proactive, technology -based fraud detection.
- Fraud-fighting activities can be grouped into three primary categories: prevention, detection, and investigation.
- Fraud detection can be categorised into technology-based and non-technology -based methods.
- Traditional fraud detection typically begins with an indication or anomaly that something isn't right, such as anonymous tips, unusual financial statement relationships, or control overrides.

- Once fraud examiners feel confident that they understand the business, they must determine what possible frauds might exist or could occur in the operation being examined.
- Fraud is a crime that is rarely seen. Rather, only fraud symptoms are observed. Unfortunately, what often appears to be a fraud symptom ends up being explained by other, non- fraud factors.
- Once symptoms are defined and correlated with specific frauds, supporting data are extracted from corporate databases and other sources.
- To effectively design and implement symptom queries, a technology expert should be part of the fraud detection team. This person must be skilled in two areas: database programming and fraud principles.
- Once relevant data are retrieved, they should be compared against expectations and models.
- Fraud examiners should follow up on all identified symptoms. While finding fraud is certainly the primary objective of follow up efforts, the process often highlights control weaknesses, ineffective systems, undocumented policies, and data errors.
- Once anomalies are highlighted and determined to be indicators of fraud, they are investigated either using traditional or technology-based approaches.
- Since much of the detection process is computerised, subsequent iterations are normally faster because analyses, algorithms, and models are already programmed
- While the team was completing the first phases of the strategic method, it concurrently worked to achieve direct access to the refinery's databases. Because of the sensitivity of these databases, the programmer was only able to gain access after convincing high-level executives why direct access was critically important.
- Once the data for a given search were stored in an appropriate warehouse, the team analysed data subsets for specified patterns. Normally, expected patterns (such as average price for specific products) were generated directly from the data rather than from outside sources.
- Exception reports, reflecting fraudulent transactions that exhibited unusual, atypical and otherwise questionable patterns of supervisor overrides, transactions with no apparent business purpose, and transactions involving unusually large amounts. This symptom came from internally used bank records and occurred at least 221 times.

## **6.0 TUTOR-MARKED ASSIGNMENT**

1. Mention the steps for a strategic detection of an electronic fraud.
2. Mention and explain briefly researches carried out in fraud detection.

## 7.0 REFERENCES/FURTHER READINGS

- AICPA. (2002). *SAS* No. 99: "Consideration of Fraud in a Financial Statement Audit Summary". AICPA.
- Albrecht, C. C., W. S. Albrecht, *et al.* 2001a. "Can Auditors Detect Fraud?: A Review of the Research Evidence." *The Journal of Forensic Accounting I*: (January-June) 1-12.
- Albrecht, C. C., W. S. Albrecht, *et al.* 2001b. "Conducting a Pro-Active Fraud Audit: A Case Study." *The Journal of Forensic Accounting II*: (June-December) 203-218.
- Albrecht, W. S. (2003). *Fraud Examination*. Mason, Ohio, South-Western.
- Blocher, E. & J. J. Willingham. (1988). *Analytical Review: A Guide to Analytical Procedures*. Shepard's/McGraw-Hill.
- Hammer. (1990). "Reengineering Work: Don't Automate, Obliterate." *Harvard Business Review*.
- Hill, T. (1996). "The First-Digit Phenomenon." *American Scientists* **86**: 358-363.
- Knapp, C. A. & Knapp, M. C. (2001). "The Effects of Experience & Explicit Fraud Risk Assessment in Detecting Fraud with Analytical Procedures." *Accounting, Organisations, and Society* **26**: 25-37.
- Nieschwietz, R. J., J. Joseph J. Schultz *et al.* (2000). "Empirical Research on External Auditors' Detection of Financial Statement Fraud." *Journal of Accounting Literature* **19**: 190-246.
- Nigrini, M. (1999). "I've Got Your Number." *The Journal of Accountancy* **187**(5).
- Palmrose, Z. (1987). "Litigation and Independent Auditors: The Role of Business Failures and Management Fraud." *Auditing: A Journal of Practice and Theory* **6**(Spring): 90-103.
- Pressman, R. S. (1997). *Software Engineering: A Practitioner's Approach*, McGraw-Hill. 270-296.
- Shelton, S., R. Whittington, *et al.* (2001). "Auditing Firms' Fraud Risk Assessment Practices." *Accounting Horizons*: 19-33.

### **UNIT 3      ELECTRONIC FRAUD DETECTION TECHNIQUES**

#### **CONTENTS**

- 1.0    Introduction
- 2.0    Objectives
- 3.0    Main Content
  - 3.1    Fraud Detection Techniques
  - 3.2    Fraud Screening Tools
  - 3.3    Internet Payment Security Methods SSL/TLS
  - 3.4    Electronic Commerce Indicator
  - 3.5    Manual Procedures
  - 3.6    One-Click Shopping
  - 3.7    SET Secure Electronic Transaction
  - 3.8    Verified By Visa
  - 3.9    MasterCard SPA/UCAF and Secure Code
  - 3.10    Maestro Payment over the Internet
  - 3.11    Transaction Liability Rules
  - 3.12    Future Trends
- 4.0    Conclusion

- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

## 1.0 INTRODUCTION

Consumer confidence and bank profits are persistently and pervasively undermined by electronic payment fraud. Over the years, fraud in card payments has increased in line with overall card volume growth, remaining at around 3% of transaction volume. Fraud tends to flow to the weakest point and, as soon as security is tightened up in one area, fraudsters are quick to move to the next point of least resistance. For example, the card organisations have developed mechanisms, such as Card Verification Value from Visa, that tackle “card present” fraud. However, there has been a rise in the level of “card-not-present” fraud in consumer channels such as Mail Order Telephone Order (MOTO) and the Internet.

Internet fraud in particular has caused many headaches for acquirers. Today, the rate of fraud for Internet purchases is up to 22 times that of card-present transactions. Such fraud levels have led acquirers servicing Internet-only merchants to seek high merchant service charge (MSC) levels or up front payments as provision for risk. Some acquirers, meanwhile, have chosen to avoid the eCommerce business completely. This has further increased costs for many Internet merchants who are already hard pressed to maintain profitability when faced with the lost time and revenues associated with fraud. Whereas an acquirer can choose not to handle Internet transactions, an issuer has little control over where the cardholder uses his card. However, despite the relatively high percentage of fraud and disputes within the Internet channel, the current low volume of Internet transactions (on average 2% of transaction volumes) has allowed issuers to manage the cost and the overall impact to their profitability. Losses from cross-border fraud and counterfeit cards are on the increase worldwide, demonstrating that fraudsters have found ways around many of today’s card-present security tools. For example, fraud from these sources is estimated to be costing UK banks up to £22 million a year. Existing physical security mechanisms used in magnetic stripe cards have been largely mastered by counterfeiters – often operating out of Far Eastern countries – allowing them to create or reproduce cards for use in both card present and card-not-present situations. The rollout of EMV chip technology is now seen as a critical short-term step in addressing such fraud. Despite the real financial pain that many merchants are experiencing, the approach of many merchants to fraud detection is haphazard, manual and uncoordinated, with under-investment in fraud prevention causing a problem throughout the whole industry.

Indeed, card organisations such as Visa have initiated programmes to identify merchants with higher than normal fraud rates with a view to applying penalties where necessary. It is growing clear to all players in the payments industry that continued growth in fraud is a real threat to revenue growth and consumer confidence. The attitude is changing from seeing fraud as an annoying but inescapable cost, to seeing fraud as a real threat to profitability that must be tackled head-on.

The examples of fraud prevention techniques explained in this section are based on Visa methodologies. MasterCard, American Express, JCB, Diners and Discover also use similar features on their cards – though the positioning and specifications may vary from brand to brand.

## **2.0 OBJECTIVES**

At the end of this unit, you should be able to:

- explain the different types of electronic fraud detection techniques
- differentiate the different types of techniques
- apply the techniques
- identify fraud screening tools
- identify the future trend in the development of electronic fraud detection techniques.



### 3.0 MAIN CONTENT

#### 3.1 Fraud Detection Techniques

**Hologram:** A hologram is embedded in the plastic card; it is difficult to copy. Though fraudsters are capable of creating such holograms, the quality of the reproduction is often poor.

**Photo ID:** Some issuers have taken the step of also introducing miniature photographs of the cardholder on the card. The problem with card photographs is the quality is often poor and the merchant rarely checks the photo against the person performing the transaction.

**Special Characters:** Visa and MasterCard have introduced embossed characters with a special font that indicates the brand or card product.

**Expiration Date:** In theory, the expiration date can limit the fraud potential of a stolen card i.e. it places a time limit on the validity of the card. However, in the case of a stolen card, it would be expected that the issuer would block the card soon after the theft, making the expiration date unnecessary in most circumstances as a means of controlling fraud.

**Signature Panel:** The signature panel contains a faded background with a Visa logo that discolors if the signature is erased. The presence of the cardholder signature itself is a key method of identifying that the cardholder is genuine for a card-present transaction. Comparing the cardholder signature on the panel against that on the receipt is the most commonly used method of cardholder verification used by merchant staff – and is perhaps the only method used in many instances. For card-present transactions, the cardholder signature on the receipt is used in dispute processing as a means of verifying that the cardholder participated in the transaction.

**LUHN Verification:** Most credit cards use the LUHN algorithm that ensures that individual digits in a PAN cannot be changed without being detected by electronic point-of-sale systems and bank authorisation systems.

**Ultra-Violet Printing:** Some card organisations print characters on their cards that are only visible using ultra-violet light. Merchants may use ultra-violet light emitters to verify genuine cards much as they verify the hidden characters on genuine paper currency.

**Magnetic Stripe:** The magnetic stripe on the back of the card contains magnetically encoded data that is read by electronic POS terminals and ATMs during the transaction. The magnetic stripe contains three

“tracks” of data based on ISO standards, though not all of the information or tracks are used by all card brands. The format of the data is mandated by each brand in their Operating Regulations documents, just as the other physical characteristics of the card are specified in detail. Track 1 was originally intended for use by airlines, but many electronic POS devices use it to retrieve the cardholder name for printing on receipts and statements. Track 2 is the standard track used by banks for card details. Track 3 was originally intended as a read/write track to allow the storage of account security and balance information, but is rarely used now for this purpose.

**Card Verification Numbers:** There are normally two Card Verification Numbers (CVNs) on the card – one encoded on the magnetic stripe and one on the signature panel or front of the card. The CVN on the magnetic stripe provides added security where transactions are authorized at the point-of-sale, while the printed CVN is designed to protect MOTO transactions where the CVN can be quoted to the merchant over the phone by the cardholder or keyed into a web page. Visa, MasterCard and American Express differ in terms of the naming and specification of the CVNs on their cards.

**Hot Card Lists:** Once the issuer is informed by the cardholder that their card is missing, the issuer will block the card within his authorisation system, and may request either Visa or MasterCard to block the card on their switching or stand-in authorisation systems. The card organisations also produce lists of cards that have been compromised and distribute these to acquirers for passing on to merchants. The Visa Card Recovery Bulletin (CRB) is an example of such a list. These lists are published on a geographic basis i.e. the issuer and card organisation will determine which regions are a high risk for a stolen card to be used.

In offline merchant environments, acquirers often choose to issue their merchants with electronic “hot card files” which are automatically downloaded into POS terminals each day when the end of day data capture or reconciliation process is triggered. This ensures that each transaction is automatically checked against the list of the most current and high-risk hot-listed cards before being sent for authorisation, so that stolen cards may be rejected even if the transaction is below floor limit.

**Online PIN:** Online verification of a four digit PIN is mandatory for all ATM transactions, and is used for debit transactions in many parts of the world. This involves the PIN data being encrypted and transmitted to the issuer for verification. As mentioned previously, the use of mandatory PIN verification at ATMs has been highly effective leading to very low rates of fraud for ATM transactions. For these transactions, the four-digit PIN is encrypted and transmitted to the issuing bank for

verification. Online PIN for debit cards (such as Maestro and Visa Debit) is very effective in combating debit fraud in some markets, though it is not used in all markets for credit card purchases.

**Address Verification Service:** The Address Verification Service is offered by card organisations in the US and UK for MOTO and Internet transactions. AVS checks the shipping address provided by the purchaser against the billing address used on the payment card. The AVS Service relies on the availability of postal codes within a country that have a strictly defined format and have a low level of granularity with respect to street addresses. In the US, such postal codes are known as ZIP codes. When making a purchase, the consumer is asked to provide his postal or ZIP code and this is included in the online authorisation request by the merchant. The postal code is verified in real time by the card organisation's switching system against the postal code registered by the issuer for each cardholder. In some instances, the merchant may choose to ship the goods to an address other than the credit card billing code if they have an outstanding relationship with the customer. The AVS Service has been available in the US for many years and has been more recently introduced in the UK. It has been shown to be extremely effective in the US at combating MOTO fraud for non-card present transactions.

**Chip Cards:** Chip technology represents the most effective medium-term solution to card fraud. Despite the compelling technological advantages of smart cards, the technology has been slow to take off, primarily because of the cost and complexity of chip implementation. In the US, where 90% of all transactions are authorised online, fraud is not the catalyst for smart card adoption. However in Europe, where telecommunications costs make online authorisations prohibitively expensive, chip has a viable business case. In Western Europe a mandated deadline has been set of January 2000 by which time acquirers must support chip & PIN and whereby the liability for fraud shifts to the issuer for chip and PIN transactions. Up to this point, PIN verification for ATM and POS transactions has involved the PIN-block information being encrypted via DES or Triple-DES and transmitted all of the way to the issuer, but Chip cards allow the PIN to be verified "offline" against the chip itself. The mandate is that basic credit and debit must be supported with offline PIN, though issuers are free to introduce value-added features, such as purse or loyalty if they choose to do so.

France was the first country to implement chip technology in 1987. In its first year of operation, the Cartes Bancaires system successfully reduced fraud by 50% despite a sizeable increase in card volume. One of the challenges facing the mandated migration to chip in Europe was

the lack of international interoperability. When tourists use foreign non-chip cards in France, or French cards are used abroad in countries where the chip is not read, then fraud levels increase to match levels in other countries. Fortunately, thanks to the efforts of the card organisations, all the major schemes, including Cartes Bancaires, have adopted the international EMV standard, ensuring global interoperability.

Some issuers and acquirers are still concerned about the cost of introduction of chip cards into the market. Issuers will need to bear the cost of basic chip cards or invest in higher capacity chip cards if they plan to support multiple applications. Initially some subsidies may be available to them from the card organisations for such cards. But acquirers must shoulder the largest burden of cost, having to upgrade all of their networks of ATMs and merchant PoS terminals to accept chip cards. Though acquirers and even card organisations are willing to make investments in their largest merchant chains and high volume merchants, the mid-to-low end merchants may themselves have to pay the cost of upgrading their own equipment. Those merchants who fail to upgrade may experience increased fraud levels as fraudsters seek out the lowest point of resistance. The most significant factor that will contribute to critical mass of adoption of chip cards is a significant recent rise in card-present cross-border fraud due to counterfeit and skimmed cards. Cross-border fraud is estimated to be costing up to \$16 million per annum in the UK alone, and is being experienced by a number of European countries. In Europe, the card organisations are promoting fraud reduction as the key business driver for chip introduction.

In the US, the 2005 mandate does not apply and the business case for chip introduction is weaker because of the lower levels of fraud experienced there. However, value-added and loyalty services and, to a lesser extent, stored value purse may be seen as the business drivers. Currently, approximately 12 million Visa-branded chip cards have been issued in the US and POS acceptance of EMV is growing. Even despite the weaker business case, regular upgrades to POS systems have ensured the EMV chip acceptance in the US is over 50%.

The introduction of chip cards is targeted at reducing the levels of fraud for card-present transactions, but it has the potential to be used for Internet purchases also when technology and standards are in place. In particular, it is likely that offline PIN authentication will be adopted in time as part of the 3-D Secure standard once chip cards are in the hands of the majority of cardholders.

### **3.2 Fraud Screening Tools**

Merchants have introduced screening tools to detect fraud – particularly in the MOTO and Internet space. In the merchant area, tools such as these will help merchants to differentiate low risk business from repeat customers or for low risk goods, versus higher risk transactions from new customers, overseas customers or where particular circumstances of the transaction represent increased risk. Many customers who shop from common MOTO stores such as flower shops or theatre ticket bookings will notice that some merchants request the consumer to provide some personal information – such as a phone number or address – which they can use for comparison purposes the next time the same payment card is presented for payment.

Acquirer fraud screening tools may detect cardholder fraud, but their primary goal is to protect the acquirer from fraudulent merchants who may “disappear” following receipt of payment from the acquirer. Such screening tools will establish trends and patterns of transaction volumes, amounts and types for each merchant or category of merchant, and compare new transactions to those patterns. Issuers have traditionally performed “velocity checking” on incoming authorisation requests to identify transactions which are unusual with respect to cardholders’ spending patterns. Such verification routines have often been included within an issuer’s core authorisation host system. Examples of such checking are –

- First use of a newly issued card – some issuers may issue Referral responses in such cases to ensure that the genuine cardholder did receive the physical card (unless the cardholder first activated his new card by phoning his bank);
- Maintenance of rolling 3 or 4 day average spending, and identification of transactions which raise that average spend above a certain threshold;
- Monitoring of what types of goods (by Merchant Category Code) the cardholder usually buys, and identifying transactions which are outside his normal types of purchases;
- Identification of transactions above his normal spend for an individual purchase;
- Identification of purchases for a cardholder originating from a country where he does not normally do business.
- Identification of (non-Internet) purchases for a cardholder originating from different geographic locations within a narrow time interval.

Issuers will use these factors together with other risk measurements related to the cardholder to make a judgment on each transaction.

In addition to these velocity checks, some issuers employ more extensive fraud screening tools to track transactions, identify trends and provide alerts on anomalies.

Patterns of expenditure for each cardholder will be established based on variables such as the types of goods purchased, high and low amounts of purchases over periods of time, geographic areas in which purchases have been made, normal frequency of card usage and other parameters. The tools will normally store transaction data over several months and identify complex patterns based on this data, which would not be apparent when examining a limited number of transactions.

Issuers may choose to implement such systems in real-time or deferred i.e. in real time the authorisation request may be declined if fraud is detected, whereas in deferred mode the potential fraud is not identified until after the authorisation request has been processed. Generally, real-time authorisation controls are more costly to implement and issuers are wary about slowing down the response time to authorisation requests if the system performance of the fraud -screening tool does not match that of their authorisation host. However, delayed fraud detection means that only future transactions may be blocked for the compromised card since the transaction has been approved and the merchant has received a valid approval code.

### **3.3 Internet Payment Security Methods SSL/TLS**

SSL (Secure Socket Layer) and TLS (Transport Layer Security) are commonly used to secure data traveling over open (Internet) networks. The goal of the TLS protocol is to provide privacy and data integrity between two communicating applications. Symmetric cryptography is used for data encryption e.g., DES, RC4, etc. to ensure that the connection is private. Message transport, using a keyed Message Authentication Code (MAC), ensures that the connection is reliable and has not been tampered with. SSL and TLS are layered on top of the standard TCP/IP protocol. SSL is frequently used by home banking web sites to secure account information displayed to customers on web pages.

### **3.4 Electronic Commerce Indicator**

The Electronic Commerce Indicator (ECI) is a value within a financial card payment authorisation request that informs the issuer of the card that the transaction has been carried out over the Internet, and whether any security protocol such as SSL, Verified by Visa, etc. were used to protect the transaction. It is mandated that all Internet transactions should have this value populated in the authorisation request. Prior to this mandate coming into effect, it was very difficult for issuers to

identify which transactions were eCommerce transactions and which were physical world transaction, and the presence of this value now makes it possible for issuers to target eCommerce transactions with fraud detection software analysis.

### **3.5 Manual Procedures**

Many small-to-medium merchants cannot afford to implement software-based fraud screening tools and must resort to manual procedures. If the customer is from within the merchant's country then the merchant may make use of locally available electoral registers or phone books to verify that the shipping address of the goods provided by the consumer corresponds to his home address. Merchants may also attempt to contact the cardholder directly using his publicly available phone number to verify that he did carry out the transaction, before shipping the goods. In some extreme cases, merchants have been known to refuse to process orders from overseas customers because their identity cannot be verified, but this practice is frowned on by the card organisations.

A recent report on fraud from CyberSource has indicated that in the US many merchants' approach to fraud detection is ad-hoc, uncoordinated and is not integrated into the merchant's operational procedures. This means that staff who are not trained to detect fraud properly will either fail to detect high-risk transactions or may lose customers by highlighting false positive fraud occurrences. In either case, valuable time is often wasted and the rate of fraud detection is unreliable.

### **3.6 One-Click Shopping**

In recent years, a number of Internet merchants have implemented "One-Click" shopping. Its goal is two-fold – both to provide ease and convenience to the online shopper, and to reduce fraudulent transactions. Using the One-Click approach, a consumer will be asked to register his personal details with an individual merchant – including his payment card details. When the consumer returns to carry out a transaction, he only has to sign-on with his username and password in order to pay for the goods, since his payment details will be picked up automatically from the database.

In many cases, the entry of only a password is required, since the merchant site will identify the user by picking up a cookie previously stored on his personal computer.

For the online merchant, the benefit is that a database will be built up over time of reliable repeat customers who carry low risk when making a purchase. This allows the merchant to focus his fraud detection

attention on new customers who have just registered, or those customers who have avoided registration and gone directly to the payment page. However, such databases must be protected by encryption and strong firewalls.

### **3.7 SET Secure Electronic Transaction**

The SET standard was launched jointly by Visa International and MasterCard in 1996 as a global standard to reduce fraud in Internet commerce. The goal of the standard was to authenticate all parties to a transaction and to secure the integrity of the transaction details using strong public key cryptography. A number of pilots were undertaken throughout the world between 1997 and 2001, but the standard did not reach the critical mass needed for adoption. The “burst bubble” in Internet stocks in 2000 also served to delay spending by many banking institutions in authentication infrastructures for Internet commerce. Both Visa and MasterCard began to work independently on the next generation of authentication mechanisms, leading to the emergence of the 3-D Secure protocol and the SPA UCAF standard from Visa and MasterCard respectively.

### **3.8 Verified By Visa**

In late 2000, Visa USA issued a technical specification for a consumer authentication protocol known as “Payer Authentication”. This was based on the concept of separating the transaction process into 3 separate domains – issuer, acquirer and message interchange. During the course of 2001 and 2002 the protocol was rolled out to other Visa regions and was given the brand name “Verified by Visa” (VbV).

The goal of Verified by Visa is to authenticate the consumer using a designated authentication code. Unlike the SET specification, Verified by Visa does not attempt to include or replace the traditional authorisation methods. Verified by Visa authentication is merely an additional step that happens before the transaction authorisation takes place, and therefore is easier for merchants to integrate into their business processes. Also, the basic protocol is much simpler than that developed for SET transactions.

The solution involves the deployment of a software module called a Merchant Plug-In (MPI) at the merchant site or his acquirer’s site (if the acquirer hosts the MPI). The issuer also needs to operate an Access Control Server (ACS) that interacts with the merchant’s MPI via XML messages over the Internet. The other two software components in the process are the Visa Directory which allows merchant MPI’s to communicate with issuer ACSs, and the Authentication History Server



which is also operated by Visa and stores a log of all fully completed authentications.

The transaction process is carried out in the following way:

- The cardholder enrolls for the Verified by Visa (or MasterCard SecureCode) service at his issuing bank and chooses his Personal Assurance Message and authentication password or PIN.
- The cardholder shops for goods and enters his payment details into the merchant checkout page as normal.
- The merchant 3-D Secure software checks with the Visa (or MasterCard) Directory and the issuer to determine whether the cardholder is enrolled for 3D secure.
- Provided that the cardholder is enrolled for the service, the merchant seeks authentication of the cardholder by his issuing bank.
- The cardholder is presented with a web page by his issuing bank that shows the details of the transaction and his Personal Assurance Message and is requested to enter his 3-D Secure password or PIN.
- The issuing bank validates the password or PIN against the details stored for the cardholder at the time of enrolment.
- The issuer responds to the merchant to indicate whether the cardholder is authentic or not, and if so, provides an authentication code to the merchant to include with the financial authorisation request.

### **3.9 MasterCard SPA/UCAF and Secure Code**

Soon after Visa launched the 3-D Secure protocol concept, MasterCard followed with a standard known as Secure Payment Application/Universal Cardholder Authentication Field (SPA UCAF). The goal of SPA/UCAF was similar to that of VbV i.e. to authenticate a cardholder prior to the event of a financial transaction. However, the technical approach taken by SPA/UCAF differed to 3-D Secure. Whereas 3-D Secure involved the flow of XML messages over the Internet between merchant and issuer, the SPA/UCAF technical approach was to assume that the cardholder would use a consumer wallet application to interact with hidden fields located on the merchant's payment pages. The wallet application would extract merchant and transaction details from the specified hidden fields and the wallet would populate data – the UCAF value generated by the issuer for example – into the hidden fields on the payment page. At this point, the additional authentication data would be passed into the merchant's payment application and sent as part of the financial authorisation message to the issuing bank. Thus, the two standards mainly differed in terms of *how* the transaction data would be transported between the merchant and the issuer. In September 2002, MasterCard announced the launch of the MasterCard SecureCode standard that could interoperate

with the 3-D Secure protocol, as well as the previously published wallet-based standard. This announcement reunited the two major brands in the use of a common technology standard for consumer authentication and paved the way for dual-brand issuers and acquirers to implement a single software solution to support both brands.

### **3.10 Maestro Payment over the Internet**

In the summer of 2001, Maestro introduced an authentication standard built upon the previously published MasterCard SPA/UCAF standard. The goal of the Maestro standard was more than just consumer authentication – it was intended to allow Maestro debit cards to be used generally for purchases over the Internet. The Maestro standard promoted the use of a pseudo-PAN and described mechanisms for both acquirers and issuers to work around for the absence of PIN-block data for Internet transactions, which is normally present for card-present transactions.

### **3.11 Transaction Liability Rules**

Traditionally, the liability rule for Internet transaction has been that the merchant takes the liability for fraudulent transactions. Hence, the merchant is in the position that he must prove that the cardholder committed fraud or assume the loss. This mirrored the rules applied to MOTO transactions, given that the same lack of direct involvement applied between the cardholder and the merchant. This rule has left many merchants considerably at risk of fraud losses, with the intention of sensitising them to implement fraud detection and prevention measures.

With effect from April 2002 in the EU region and April 2003 in all other regions, Visa has mandated that, under certain conditions, fraud liability shifts to the issuer in instances where the Internet merchant has adopted the Verified by Visa protocol. Effectively, this means that Internet merchants who implement the VbV merchant-plugin will be protected from fraud, moving the focus from the merchant/acquirer to the issuer to prevent fraud. This is intended to incentivise issuers to properly authenticate their cardholders to avoid financial loss. MasterCard has introduced similar liability shift for those merchants implementing SecureCode.

### **3.12 Future Trends**

The following are a series of predictions with respect to fraud -related events over the coming decade:

1. Despite the risks of fraud outlined in this unit, the credit/debit card will remain the safest and most secure means for consumers to make payments, particularly over the Internet. The degree of protection provided to consumers by the regulations mandated by card schemes such as Visa and MasterCard are unmatched by other payment methods. This will ensure the continued growth of card payments.
2. The introduction of EMV chip cards will have little or no affect on MOTO fraud.
3. Eventually fraudsters may find a way to cost-effectively skim and create counterfeit chip cards, and the move to strengthen card security will begin again. The next step up in security will most likely take the form of biometrics – using technology such as fingerprints, voice analysis or retinal scans.
4. The volume of Internet transactions secured by Verified by Visa and MasterCard SecureCode will grow steadily as Internet transaction volumes and the global economy improves.
5. The single greatest threat that will continue to raise its head this decade is the growth of identity theft. As a result of the introduction of more computerised systems in many consumer-facing institutions, there is more personal information available on individuals in electronic (and hence easily distributed) format. Indeed, if a person were to wish to truly protect their personal information in their day-to-day lives, then they may be unable to avail of a wide number of services from banks, insurance agencies, employers and merchants who all require that such information be provided to them.

Protection will be unlikely to be provided to citizens until Government action is taken to regulate the use and storage of such information, and to provide a secure form of personal authentication from birth. The debate on the ownership of personal information and evidence of identity is likely to be one of the most significant and important this decade, with long lasting implications for the future.

#### **4.0 CONCLUSION**

The negative impacts of fraud on financial and other forms of transactions informed concerned organisations to develop technologies to counter fraudulent schemes. Though these techniques are not totally full proof they have gone a long way in deterring fraudsters. As

technologies advance more potent techniques will be developed and deployed to secure business transactions globally.

## 5.0 SUMMARY

- Consumer confidence and bank profits are persistently and pervasively undermined by electronic payment fraud. Over the years, fraud in card payments has increased in line with overall card volume growth, remaining at around 3% of transaction volume.
- A hologram is embedded in the plastic card, that is difficult to copy. Though fraudsters are capable of creating such holograms, the quality of the reproduction is often poor.
- The signature panel contains a faded background with a Visa logo that discolours if the signature is erased. The presence of the cardholder signature itself is a key method of identifying that the cardholder is genuine for a card-present transaction.
- The magnetic stripe on the back of the card contains magnetically encoded data that is read by electronic POS terminals and ATMs during the transaction.
- Online verification of a four digit PIN is mandatory for all ATM transactions, and is used for debit transactions in many parts of the world. This involves the PIN data being encrypted and transmitted to the issuer for verification
- Chip technology represents the most effective medium-term solution to card fraud. Despite the compelling technological advantages of smart cards, the technology has been slow to take off, primarily because of the cost and complexity of chip implementation
- Merchants have introduced screening tools to detect fraud – particularly in the MOTO and Internet space
- SSL (Secure Socket Layer) and TLS (Transport Layer Security) are commonly used to secure data traveling over open (Internet) networks.
- The Electronic Commerce Indicator (ECI) is a value within a financial card payment authorisation request that informs the issuer of the card that the transaction has been carried out over the Internet, and whether any security protocol such as SSL, Verified by
- Visa, etc. were used to protect the transaction
- Many small-to-medium merchants cannot afford to implement software-based fraud screening tools and must resort to manual procedures.
- In recent years, a number of Internet merchants have implemented “One-Click” shopping. Its goal is two-fold – both to provide ease and convenience to the online shopper, and to reduce fraudulent transactions.

- Both Visa and MasterCard began to work independently on the next generation of authentication mechanisms, leading to the emergence of the 3-D Secure protocol and the SPA UCAF standard from Visa and MasterCard respectively.
- In late 2000, Visa USA issued a technical specification for a consumer authentication protocol known as “Payer Authentication”. This was based on the concept of separating the transaction process into 3 separate domains – issuer, acquirer and message interchange
- Soon after Visa launched the 3-D Secure protocol concept, MasterCard followed with a standard known as Secure Payment Application/Universal Cardholder Authentication Field (SPA UCAF).
- Traditionally, the liability rule for Internet transaction has been that the merchant takes the liability for fraudulent transactions.
- Despite the risks of fraud outlined in this unit, the credit/debit card will remain the safest and most secure means for consumers to make payments, particularly over the Internet

## 6.0 TUTOR-MARKED ASSIGNMENT

1. Mention 10 techniques used in fraud detection.
2. Discuss briefly, the USA Visa **Payer Authentication** transaction process.

## 7.0 REFERENCES/FURTHER READINGS

CyberSource Online Fraud Report (2002). (Conducted by Mindwave Research).

CNET News

David Guerin, (2003). *Fraud in Electronic Payment*, Trintech Group Plc.

## **UNIT 4      CONTROL AND AUDITING OF INFORMATION   SYSTEM**

### **CONTENTS**

- 1.0    Introduction
- 2.0    Objectives
- 3.0    Main Content
  - 3.1    Security and the Role of Controls
  - 3.2    Defense Strategies and How to Protect
  - 3.3    General and Application Control
    - 3.3.1   General Controls
    - 3.3.2   Application Controls
  - 3.4    Implementing Controls
  - 3.5    Purpose of Audit
  - 3.6    History of IT Audit
  - 3.7    Types of Auditors and Audits
  - 3.8    How is Audit Executed?
  - 3.9    Sources of Information for Auditors Reports
  - 3.10   A Case of Authorised Hackers Breaking into a System
- 4.0    Conclusion
- 5.0    Summary
- 6.0    Tutor-Marked Assignment
- 7.0    References/Further Readings

### **1.0    INTRODUCTION**

Controls are established to ensure that information systems work properly, for example, in electronic banking system. Controls can be installed in the original system: information system department, end-users, or others (e.g. vendors) can add them once a system is in operation. Installing controls is necessary but not sufficient. It is also necessary to answer questions such as the following: Are controls installed as intended? Are they effective? Did any breach of security occur? If so, what actions are required to prevent reoccurrence? These questions need to be answered by independent and unbiased observers. Such observers perform the information system auditing task.

An audit is an important part of any control system. In an organisational setting, it is usually referred to as a regular *examination* and *check* of financial and accounting records and procedures. Specially trained professionals who may be internal employees or external consultants execute auditing. In the information system environment, auditing can be viewed as an additional layer of controls or safeguards.

## 2.0 OBJECTIVES

At the end of this unit, you should be able to:

- explain why controls are designed
- identify types of control and defense strategies
- mention some biometric controls
- answer question on how to implement controls.
- explain the purpose of conducting a system and information technology audit
- identify the types of audit carried on a system, as well as types of auditors
- explain how audit is conducted
- state how to source information for audit reports.

## 3.0 MAIN CONTENT

### 3.1 Security and the Role of Controls

Protection of information technology is accomplished by inserting controls that is, defense mechanisms intended to *prevent* hazards, *deter* problems as early as possible, *enhance damage recovery* and *correct problems*. Controls can be integrated into hardware and software during the systems development phase (a most efficient approach). They can also be implemented once the system is in operation or during maintenance. The important point is that defense should stress *prevention*; it does no good after the crime. Since there are many threats, there are also many defense mechanisms. In this unit we describe some representative controls.

Controls are designed to protect all the components of an information system, specifically data, software, hardware, and networks.

### 3.2 Defense Strategies and How to Protect

The selection of a specific strategy depends on the objective of the defense and the perceived cost-benefit.

The following are the major defense strategies:

- **Control for Prevention and Deterrence.** Properly designed controls may prevent errors from occurring, deter criminals from attacking the system, and better still, deny access to unauthorised people. Prevention and deterrence are especially important where the potential damage is high.

- **Detection.** It may be economically feasible to prevent all hazards, and deterring measures may not work. Therefore, unprotected systems are vulnerable to attack. Like a fire, the earlier it is detected, the easier it is to combat and the less the damage. Detection can be performed in many cases by using special diagnostic software.
- **Limitation.** This means to minimise losses once a malfunction has occurred. Users typically want their systems back in operation as quickly as possible. This can be accomplished by including *fault-tolerant system* that permits operation in a degraded mode until full recovery is made. If a fault tolerant system does not exist, a quick (and possibly expensive) recovery must take place.
- **Recovery.** A recovery plan explains how to fix a damaged information system as quickly as possible. Replacing rather than repairing components is one route to fast recovery.
- **Correction.** Correcting damaged systems can prevent the problem from occurring again.

### 3.3 General and Application Control

Information system control can be divided into two major groups: general (system) controls and application controls. **General controls** are established to protect the system regardless of specific application. For example, protecting hardware and controlling access to the data center are independent of the specific application. **Application controls** are safeguards that are intended to protect specific applications.

#### 3.3.1 General Controls

The major categories of general controls are physical controls, access controls, data security controls, communication (network) controls, and administrative controls.

1. **Physical Control:** Physical security refers to the protection of computer facilities and resources. This includes protecting physical property such as computers, data centers, software, manuals, and networks. Physical security is the first line of defense and usually the easiest to construct. It provides protection against most natural hazards as well as against some human hazards. Appropriate physical security may include several controls such as the following:
  - (i) Appropriate design of the data center. For example, the site should be non-combustible and waterproof.



- (ii) Shielding against electromagnetic fields.
- (iii) Good fire prevention, detection, and extinguishing systems, including sprinkler system, water pumps, and adequate drainage facilities. A better solution is fire-enveloping Halon gas systems.
- (iv) Emergency power shutoff and backup batteries, which must be maintained in operational condition.
- (v) Properly designed, maintained, and operated air-conditioning systems.
- (vi) Motion detector alarms that detect physical intrusion.

**2. Access Controls:** Access control is the restriction of unauthorised user access to a portion of a computer or to the entire system. To gain access, a user must first be *authorised*. Then when the user attempts to gain access, he or she must be *authenticated*. Access to a computer system basically consists of three steps:

- (i) Physical access to a terminal
- (ii) Access to the system
- (iii) Access to specific commands, transactions, privileges, programs, and data within the system.

Access control software is commercially available for large mainframes, minicomputers, personal computers, local area networks, and dial-in communications networks. Access control to the network is executed through firewalls.

Access procedures match every valid user with unique user identifier (UID). They also provide authentication method to verify that users requesting access to the computer system are really who they claim to be. User identification can be accomplished when the following identifies each user:

- Something only the user *knows*, such as password.
- Something only the user *has*, for example, smart card or token.
- Something only the user *is*, such as signature, voice, fingerprint, or retinal (eye) scan. It is implemented via biometric controls.

A **biometric control** is defined as an “automated method of verifying the identity of a person, based on physiological or behavioral characteristics”. The most common biometrics are the following:

- i. Photo:** The computer takes a picture of your face and matches it with a pre-stored picture. In 1997, this method was successful in correctly identifying users except in cases of identical twins.

- ii. **Fingerprints:** Each time a user wants access, matching a fingerprint against a template containing the authorised person's fingerprint identifies him or her.
  - iii. **Hand Geometry:** Similar to finger prints except the verifier uses a television-like camera to take a picture of the user's hand. Certain characteristics of the hand (e.g. finger length and thickness) are electronically compared against the information stored in the computer.
  - iv. **Blood vessel pattern in the retina of the person's eye:** A match is attempted between the pattern of the blood vessels in the back-of-the-eye retina that is being scanned and a pre-stored picture in the retina.
  - v. **Voice:** A match is attempted between the user's voice and the voice pattern stored on templates.
  - vi. **Signature:** Signatures are matched against the pre-stored authentic signature. This method can supplement a photo-card ID system.
  - vii. **Keystroke dynamics:** A match of the person's keyboard pressure and speed against pre-stored information.
  - viii. **Others:** Several other methods exist such as *facial thermo-graph iris* and *scan*
3. **Data Security Control:** Data security is concerned with protecting data from accidental or intentional disclosure to unauthorised persons, or from unauthorised modification or destruction. Data security functions are implemented through operating systems, security access control programs, database/data communications products, recommended backup/recovery procedures, application programs, and external control procedures. Data security must address the following issues: *confidentiality of data, access control, critical nature of data, integrity and of data.*

Two basic principles should be reflected in data security:

- **Minimal Privilege:** Only the information a user needs to carry out an assigned task should be available to him or her.

- **Minimal Exposure:** Once a user gains access to sensitive information, he or she has the responsibility of protecting it by making sure only people whose duties require it obtain knowledge of this information while it is processed, stored, or in transit.

Data integrity is the condition that exists as long as accidental or intentional destruction, alteration, or loss of data *does not* occur. It is the preservation of data for its intended use.

4. **Communications (Network) Controls:** Network protection is becoming extremely important as the use of Internet, intranets, and electronic commerce increases.

5. **Administrative Controls:** While the previously discussed controls were technical in nature, administrative control deals with issuing guidelines and monitoring compliance with the guidelines. Representative examples of such control include the following:

- Appropriately selecting, training, and supervising employees, especially in accounting and information systems.
- Fostering company loyalty.
- Immediately revoking access privileges of dismissed, resigned, or transferred employees.
- Requiring periodic modification of access controls (such as passwords)
- Developing programming and documentation standards (to make auditing easier and to use the standards as guides for employees).
- Insisting on security bonds or malfeasance insurance for key employees.
- Instituting separation of duties, namely dividing sensitive computer duties among as many employees as economically feasible in order to decrease the chance of intentional or unintentional damage.
- Holding periodic random audits of the system.

6. **Other General Controls:** Several other types of controls are considered general. Representative examples include the following:

- **Programming Controls:** Errors in programming may result in costly problems. Causes include the use of incorrect algorithm or programming instructions, carelessness, inadequate testing and

configuration management, or lax security. Controls include training, establishing standards for testing and configuration management, and enforcing documentation standards.

- **Misunderstanding or misinterpretations:** Manuals are often a source of problem because they are difficult to interpret or may be out of date. Accurate writing, standardisation updating, and testing are examples of appropriate documentation control. Intelligent agents can be used to prevent such problems.
- **Systems development controls:** Systems development controls ensure that a system is developed according to established policies and procedures. Conformity with budget, timing, security measures, and quality and documentation requirements must be maintained

### 3.3.2 Application Controls

General controls are intended to protect the computing facilities and provide security for hardware, software, data and networks. However, general controls do not protect the *content* of each specific application. Therefore, controls are frequently built into the application (that is, they are part of the software) and are written as validation rules. They can be classified into three major categories: *input controls*, *processing controls*, and *output controls*.

**Input controls:** Input controls are designed to prevent data alteration or loss. Data are checked for accuracy, completeness and consistency; they prevent the GIGO (Garbage-in, garbage-out) situations. Examples of input controls are the following:

- **Completeness:** Items should be of specific length (e.g. nine digits for a Social Security number). Addresses should include a street, city, state and zip code.
- **Format:** Formats should be standard form. For example, sequences must be preserved (zip code comes after address).
- **Range:** Only data within a specific range are acceptable. For example, zip code ranges between 10,000 and 99,999, the age of person can be larger than say, 120 and hourly wages cannot exceed \$50.
- **Consistency:** Data collected from two or more sources need to match. For example, in medical history data males cannot be pregnant.

**Processing controls:** Processing controls ensures that data are complete, valid and accurate when being processed and that program has been properly executed. These programs only allow authorised users to access certain programs or facilities and monitor the computer's use by individuals.

**Output controls:** Output controls ensure that the result of computer processing is accurate, valid, complete, and consistent. By studying the nature of common output errors and causes of such errors, management can evaluate possible controls to deal with problems. Also, controls ensure that outputs are sent only to authorised person.

### 3.4 Implementing Controls

Implementing controls in an organisation can be a very complicated task, particularly in large, decentralised companies where administrative controls may be difficult to enhance. For example, Lee (1990) suggests that IT auditing be expanded to include end-user computing.

**Planning and Organizing:** A comprehensive control and security management program begins with establishment of a formal documented, organisational *secure policy* endorsed by the highest level of management in the organisation. Such a program was developed by Fine (1983). Fine's *total computer security* can be envisioned as a horizontal beam supported by nine pillars. Three of the pillars are technical issues: *physical security, control and system security*. These three support the integrity and confidentiality of an organisational information system.

The other six pillars are managerial and they are:

- A defined and documented computer security policy
- Standards and Procedures
- An assignment of responsibilities for computer security
- A personnel security program
- A complete asset-threat inventory
- Introduction of user awareness.

Each of the program's policy must be carefully planned and properly managed. This may not be a simple task, since the pillars are fairly broad.

Developing a security program begins with a detailed analysis of current equipment, functions performed, data contained, ease of access, security devices, and potential losses. Following this analysis, a policy can be drafted that will focus on employees as well as other assets (hardware,

software, and data). Any security policy developed should deal with threats proactively, not just reactively. For each identified threat, the policy should describe not only the necessary protection, but also the actions to be taken if the threats materialise. Stringent policies, surprise audits, and strenuous *security awareness* programs are excellent ways of protecting the company's information systems.

Security administration is the responsibility of both the information systems department and the line managers. Line managers are responsible for protecting all the resources in their possession and for ensuring that their subordinates are aware of and abide by established security policies and procedures.

### 3.5 Purpose of Audit

An IT audit is similar to a financial statement audit in that the study and evaluation of the basic elements of internal control are the same. However, the purpose of a financial statement audit is to determine whether an organisation's financial statements and financial condition are presented fairly in accordance with Generally Accepted Accounting Principles (GAAP). Regarding Protection-of-Information-Assets, one purpose of an IT audit is to review and evaluate an organisation's information system's availability, confidentiality, and integrity by answering questions such as:

- Will the organisation's computer systems be available for the business at all times when required? (Availability).
- Will the information in the systems be disclosed only to authorised users? (Confidentiality).
- Will the information provided by the system always be accurate, reliable, and timely? (Integrity).

### 3.6 History of IT Audit

The concept of IT auditing was formed in the mid-1960's and has gone through numerous changes due to advances in technology and the incorporation of technology into business

Auditing information security is a vital part of any IT audit. Within the broad scope of auditing information security we find topics such as data centers, networks and application security. Auditing information security covers topics from auditing the physical security of data centers to auditing the logical security of databases and highlights key components to look for and different methods used for auditing these areas. It is important to remember that in this ever expanding technical realm these things are always changing and as such IT auditors must

continue to expand their knowledge and understanding of systems and the systems environment to help verify and ensure information security.

### 3.7 Types of Auditors and Audit

There are two types of auditors and audit: internal and external.

An internal auditor is usually a corporate employee who is not a member of the information system department.

An external auditor is a corporate outsider. This type of auditor reviews the findings of the internal auditor and the inputs, processing, and output of information systems. The external audit of information systems is frequently a part of the overall external auditing performed by a Certified Public Accounting (CPA) firm.

IT auditing (which used to be called electronic data processing auditing) can be very broad, so only the essentials are presented in this unit. Auditing looks at all potential hazards, frauds and controls in information systems. Several guidelines are available to assist auditors in their jobs.

Auditors attempt to answer questions such as these:

- Are there sufficient controls in the system?
- Which areas are not covered by controls?
- Which controls are not necessary?
- Are controls implemented properly?
- Are the controls effective; that is, do they check the output of the system?
- Is there a clear separation of duties?
- Are there procedures to ensure compliance with the controls?
- Are there procedures to ensure reporting and corrective actions in case of violations of controls?

Two types of audits are used to answer these questions. The *operational audit* determines whether the information systems department is working properly. The *compliance audit* determines whether controls have been implemented properly and are adequate.

### 3.8 How is Audit Executed?

IT auditing procedure can be classified into three categories: auditing *around* the computer, auditing *through* the computer, and auditing *with* the computer.

*Auditing around the computer* means verifying processing by checking for known outputs using specific inputs. , Therefore it is assumed that there is need to check the processing if the correct output is obtained. The best application of this approach is in systems that produce a limited range of outputs. It is fast and inexpensive, but it may give the false result. For example, two errors may compensate for each other, resulting in correct output.

In *auditing through the computer* inputs, outputs, and processing are checked. This approach is more complex and is usually supported by special tools. Some methods used by auditors are reviewing program logic, test data, and controlling processing and reprocessing.

*Auditing with the computer* means using a combination of client data. It allows auditor to perform tasks such as simulating payroll program logic using live data.

Auditors use several tools to increase their effectiveness and efficiency. Typical tools are check tools, formulas, and charts. This can be executed manually or computerised. Several computer programs are available to support the auditor's job. These include programs for testing, summarising sampling, and matching. Generalised audit software (GAS) is a set of programs designed to support auditing. Expert systems and neural computing also can be used to facilitate IT auditing.

### 3.9 Sources of Information for Auditors Reports

Auditors gather information from sources such as samples of inputs and outputs, interviews with end users and information systems employees, application program tested using the auditor's data and review of previous audit reports. Audit reports are presented in special reports submitted to the audit committee. These reports call attention to weaknesses and deficiencies and suggest possible remedies. They also highlight positive aspects of the system.

Often, it is necessary to trace a transaction through each processing step (when, where, by whom, and so on) the procedure (or document) that describes such tracing is called **audit trail**. In manual systems it is fairly easy to conduct an audit trail. However, in computerised systems, this may not be so easy. One task of auditing is to provide procedures for audit trail and to execute them when needed.

Auditors and security consultants may try to break into a computer system, in what is called a *simulated attack*, in order to find weak points in the system. In some cases companies hire hackers to do the job.



### 3.10 A Case of Authorised Hackers Breaking into a System

Auditors for the State of Illinois issued a public statement on July 1, 1993, in which they notified the State that they were successful in their mission of breaking into the Central Computer Facility which serves 109 state agencies. The auditors pulled off their mission with “disturbing ease”. An authorised hacker operating from a remote location, was able to break into the system, and read, modify, and delete data such as payroll and prison records. Real hackers could have altered the security structure and negated systems integrity. The security system, which was thought to be satisfactory, was enhanced immediately and all known flaws were fixed.

## 4.0 CONCLUSION

Controls and audit have been important and standard tools to track, minimise and prevent frauds. These disciplines require a lot of skill, tact, patience and discipline to deliver maximally. Many organisations have depended on the strict guidelines and procedures provided by these disciplines to deal with threat of fraud. It is worthy of note that the success of control and audit rely so much on the ability of the human agents in adhering to prescribed guidelines. However, in a dynamic and electronic financial environment of today, controls and audits alone are not sufficient in dealing with ever increasing threat of fraud. A combination of other measures with controls and audit will go a long way in dealing with electronic frauds.

## 5.0 SUMMARY

- Protections of information technology is accomplished by inserting controls that is, defense mechanisms intended to *prevent* hazards, *deter* problems as early as possible, *enhance damage recovery* and *correct problems*.
- The selection of a specific strategy depends on the objective of the defense and the perceived cost-benefit.
- Information system control can be divided into two major groups: general (system) controls and application controls. **General controls** are established to protect the system regardless of specific application.
- Physical security refers to the protection of computer facilities and resources.
- Access control is the restriction of unauthorised user access to a portion of a computer or to the entire system.
- A **biometric control** is defined as an “automated method of verifying the identity of a person, based on physiological or behavioral characteristics”.

- Data security is concerned with protecting data from accidental or intentional disclosure to unauthorised persons, or from unauthorised modification or destruction.
- While the previously discussed controls were technical in nature, administrative control deals with issuing guidelines and monitoring compliance with the guidelines.
- Implementing controls in an organisation can be a very complicated task, particularly in large, decentralised companies where administrative controls may be difficult to enhance.
- Developing a security program begins with a detailed analysis of current equipment, functions performed, data contained, ease of access, security devices, and potential losses
- An IT audit is similar to a financial statement audit in that the study and evaluation of the basic elements of internal control are the same
- The concept of IT auditing was formed in the mid-1960's and has gone through numerous changes due to advances in technology and the incorporation of technology into business
- An internal auditor is usually a corporate employee who is not a member of the information system department.
- IT auditing procedure can be classified into three categories: auditing *around* the computer, auditing *through* the computer, and auditing *with* the computer.
- Auditors gather information from sources such as samples of inputs and outputs, interviews with end users and information systems employees, application program tested using the auditor's data and review of previous audit reports
- Auditors for the State of Illinois issued a public statement on July 1, 1993, in which they notified the state that they were successful in their mission of breaking into the Central Computer Facility which serves 109 state agencies.

## **6.0 TUTOR-MARKED ASSIGNMENT**

1. Briefly categorise information technology audit procedures.
2. Mention five representative examples of administrative controls.

## **7.0 REFERENCES/FURTHER READINGS**

Turban, E., Mclean E., & Wetherbe, J. (1999). *Information Technology Management*. Juan Wiley & Sons Inc.

## **UNIT 5      GUIDELINES FOR ELECTRONIC/INTERNET BANKING AUDIT PROGRAM**

### **CONTENTS**

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
  - 3.1 Preliminary Procedures
  - 3.2 Prior Audit and Examination Reports
  - 3.3 Internet Banking Products and Services
  - 3.4 Implementation
  - 3.5 Policies and Procedures
  - 3.6 Administration
  - 3.7 Accounting and Processing
  - 3.8 Legal and Regulatory Matters
  - 3.9 Conclusion Procedures
  - 3.10 Policies and Procedures
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

### **1.0 INTRODUCTION**

Guidelines for electronic Internet banking are sets of rules, codes and procedures that must formally, be adhered to in the course to executing electronic banking process. These guidelines are audits to forestall fraud, abuse and inefficiency in electronic financial transactions. The audit program remains a guide whose effectiveness is dependent on how it is being implemented by human beings.

The objectives of this audit are:

- To gain an understanding of the bank's Internet banking product line, transaction flow and settlement processes.
- To ensure that adequate internal controls are in place to minimise errors, discourage fraud, and provide an adequate audit trail.
- To determine whether the board of directors has adopted effective policies for Internet banking and these policies and procedures are being followed.
- To determine if contingency and disaster plans are adequate.
- To determine if the bank complies with applicable regulations.
- To determine whether management has instituted controls that are appropriate to the type and level of risks arising from Internet banking.

## **2.0 OBJECTIVES**

At the end of this unit, you should be able to:

- explain the preliminary procedure of conducting an electronic/Internet banking audit
- state the documents to obtain prior to conducting an audit e-banking.
- identify the sectors of Internet/e-banking that need to be audited
- explain how to audit policies and procedures in the e-banking sector
- explain how to deal with legal and regulatory matters in the Internet auditing process.

## **3.0 MAIN CONTENT**

### **3.1 Preliminary Procedures**

1. Obtain a current list of the personnel who work in the Internet Banking Department, including their duties.
2. Obtain or prepare a flow chart and/or narrative detailing the Internet banking system.
3. Obtain the following documentation prior to the audit:
  - Summaries of strategic plans.
  - Independent reviews, assessments, or system certifications performed by consultants or technology experts contracted by the bank. (Note any outstanding deficiencies.)
  - Information detailing Internet banking activities conducted.
  - Details regarding complaints specific to Internet banking.
  - External audit reports and related materials.
  - Summaries of relevant operating policies and procedures.
4. Determine whether external vendors are used and what services or products are provided. Identify documents responsible for development, operation, and/or support of the Internet banking system.
5. Review documentation and conduct discussions with management to determine:
  - How security for Internet banking is addressed.
  - How management supervises Internet banking functions, including outsourced functions.
  - Any significant changes in policies, practices, personnel, or control systems.
  - Any internal or external factors that could affect the Internet banking area.
6. Gain an understanding of the bank's Internet banking business and disclosures by reviewing the bank's web site.

7. Prepare a general ledger balance comparison for all general ledger accounts related to Internet banking. Obtain an explanation for all large differences.

### **3.2 Prior Audit and Examination Reports**

1. Review the prior audit report and note items to be followed up during the current audit. Determine if management has taken appropriate and timely action to address the deficiencies noted in the audit report.
2. Review any examination reports received since the last audit. Determine if management has taken appropriate and timely action to address any deficiencies noted.

### **3.3 Internet Banking Products and Services**

1. Obtain a description and/or diagram of the Internet banking system and its capabilities. Consider hardware, software, points of connectivity to internal systems, and remote access points. Evaluate:
  - How the Internet banking system is linked to other host systems or the network infrastructure in the bank.
  - How transactions and data flow through the network.
  - Potential areas of vulnerability.
2. Obtain an overview of transaction and payment services flow and settlement processes and determine whether:
  - The bank's settlement responsibilities are clearly defined.
  - The vendor's policies address uncollected funds, settlement, customer service, backup, contingency planning, and disaster recovery.
3. Review the transaction and payment services products. Determine whether adequate control features are built into the systems to ensure authentication of the user, data integrity, and confidentiality of transactions.
4. Review any web linking relationships with both affiliated and unaffiliated third parties. Ascertain if sufficient due diligence was conducted on the third parties with which we formed web linking relationships with respect to their ability to provide service and their overall information security and privacy policies.

- Ensure formal contracts or agreements were negotiated that define the rights and responsibilities of the bank and third parties.
- Determine if appropriate disclosures are displayed on the bank's website so that customers are not confused about which products and services are offered by the bank and which are offered by third parties in web linking relationships. (OCC Bulletin 2001 31)

### **3.4 Implementation**

1. Determine whether the board, or an appropriate committee, approved the Internet banking system based on a written strategic plan and risk analysis.
2. Determine if management provides adequate training for all officers and staff affected by electronic banking systems, including those responsible for products, services, information systems, compliance, and legal issues.

(Note: The training program should be ongoing).

3. Determine if management verifies the accuracy and content of financial planning software, calculators, and other interactive programs (between the bank and its customers) available through the systems.

### **3.5 Policies and Procedures**

1. Determine whether the bank has established policies over hypertext links that enable consumers to clearly distinguish:
  - Insured and non-insured financial products.
  - Bank versus non-bank products.
  - When leaving the bank's Web site.
2. Determine if policies and procedures governing access to and the disclosure of customers' confidential information are updated for electronic capabilities.
  - Determine if the policies address what information may be shared with third parties such as non-deposit product representatives, discount brokerage services, etc.
  - Determine if guidelines pertaining to confidential information are included as part of the contracts and agreements covering third party arrangements.

3. Review a sample of Internet Banking customers and ensure they are only allowed access to accounts for which they are authorised signers.
  - Commercial accounts may have users who are not authorised signers. However, they must be approved by an authorised signer on the account.
4. Determine how management monitors system performance (e.g., transaction volume, response times, availability / downtime, capacity reports, and customer service logs and complaint summaries.)

The following provides various methods for reporting this information; determine those that would be appropriate for this organisation and detail the method in which it is reviewed.

Number of visitors to the website

- “User Assets” information
  - Number and volume of new Internet banking loans for the month
  - Number and volume of total Internet banking loans as of the end of the month□
  - Volume of total loans outside our normal servicing area
  - Volume of total deposits outside our normal servicing area
  - All security threats or repeated unauthorised access attempts
  - Any time during which the Internet banking site was non-operational for four hours or longer.
5. Determine whether Internet banking security policies include:
    - a) Clear lines of responsibility for system security - Review the duties of the security administrator. Determine if their authority is adequate to dictate controls and enforce policies.
    - b) Network and data access control.
  6. Determine whether Internet banking firewall policies address:
    - Responsibility for firewall maintenance and monitoring
    - Well-defined access rules
    - Access rules that dictate what traffic is allowed or forbidden.
  7. Determine whether encryption is adequately addressed in the security policy and the policy includes:
    - Who is responsible for control of encryption processes?
    - How encryption is used.

- Data classification techniques.
  - Use of encryption to protect transmission of passwords, messages, or data during internal and open network communications sessions.
8. Determine whether policies establish the use of virus detection software and note the products used.
  9. Identify whether security policies are periodically reviewed and updated and note whether the board of directors or senior management committee approves the policies.

### **3.6 Administration**

1. Ascertain if an Internet banking security officer has been named, as well as a backup.
  2. On a sample basis, ascertain if users of the Internet banking system have unique user IDs and passwords. Ensure passwords are changed quarterly
  3. Ensure the ISP password and master passwords are changed monthly
  4. Determine if senior management establishes appropriate levels of access to information and applications for officers, employees, system vendors, customers, and other users. Determine if the access levels are enforced and reviewed on a regular basis (annually, per policy).
- Review Employee Access to Internet Banking System forms.
5. Determine if management establishes adequate programs for customer service and support:
    - Review the organisation and responsibilities of the customer support function.
    - If the customer support service is outsourced, note the responsibilities of the vendor and determine how management monitors customer problems, demands, or complaints.
    - Determine whether customer service levels have been established. If so, determine how management monitors adherence to service levels.
    - Determine how management assesses the adequacy of customer service.
    - Determine whether deficiencies exist in the process by reviewing problem logs or customer service reports and through discussions with management.
  6. Determine if management generates and reviews exception reports on a periodic basis.



7. Tour the server location(s).
  - a) Determine if access to the console is controlled.
  - b) Determine if adequate fire detection and suppressant equipment is available.
  - c) Determine if the server is connected to an uninterruptible power supply (UPS) and whether it has been tested.
  - d) Determine that servers are protected from damage resulting from electric power surges and spikes.
  - e) Determine if housekeeping procedures are adequate to provide protection from food, liquids, dust, smoke, and magnetic fields.
8. Determine that the bank has an adequate electronic banking security program that addresses the following, as appropriate:
  - Access to, protection of, and disclosure of customers' confidential information
  - Methods for establishing the legitimacy of each party requesting an account action or submitting related instructions or data
  - What information may be shared with third-parties
  - The ability of third-party services to access or monitor electronic transmissions between the bank and any of its customers.
9. Assess the adequacy of the process for password administration for the Internet Banking System. Consider the following:
  - The adequacy of control and security over the bank's process for issuing passwords to customers.
  - Whether alphanumeric passwords are required.
  - The required length of passwords.
  - Whether passwords have an automatic expiration.
  - If adequate procedures are in place for resetting passwords.
  - If automatic log-off controls exist for user inactivity.
  - Whether excessive failed access attempts by the user disables access.
10. Ascertain if access to the Internet Service Provider (ISP) password, Master Passwords, and S1 server password is appropriate.
11. Ensure that repeated failed attempts to gain access to information result in an automatic timeout.
12. Determine whether there is a direct / indirect connection between the bank's internal operating system (s) and the system that hosts the external electronic service or activity (for example, a web site).

13. Determine if procedures exist to monitor unauthorised attempts to access the bank's system.
  - Determine if the bank's policies require formal reporting in case of attempted or actual attacks against any of the bank's systems.
  - Review all known incidents and ensure they were reported to the proper authorities.
14. Determine whether the bank has an adequate process regarding virus detection and prevention associated with the Internet banking system. Consider whether:
  - User awareness efforts address viruses.
  - The virus containment program is documented.
  - Screening for viruses uses a virus detecting software package.
  - The frequency with which anti-virus products and definitions are updated is adequate, and the most current version/release is installed.
  - Virus detection software distribution is made through downloads from the bank's server.
15. Determine whether the bank has an adequate process to address physical security for computer hardware, software, communication equipment, and communication lines associated with the Internet banking system including:
  - Whether the network servers are secured.
  - How the bank prevents unauthorised physical access to equipment.
  - Whether the bank secures vendor owned equipment.
  - If proper physical controls are in place for the data center housing equipment and documentation.
16. Determine if the bank entered formal contracts with each vendor. Determine if the contracts contain the following information and are reviewed by bank legal counsel, if appropriate:
  - Description of the work to be performed by the services.
  - Applications to be processed and services to be provided.
  - Responsibilities of both parties regarding addition or deletion of applications.
  - Processing frequency and report generation.
  - Processing priorities for both normal and emergency situations.
  - Rights, responsibilities, and liability for each party.
  - Basis of costs and description of additional fees.
  - Monthly processing fees, additional charges and free services, basis of fee calculations.

- Ownership of any special software developed for bank. (Generally, the developer owns the product.)
  - Costs for satisfying special management requests, audit needs, and regulatory requirements.
  - Price changes.
  - Online communications availability, transmission line security, and transaction authentication. – Operating hours for online communication network.
  - Responsibilities for security of the communications network
  - Audit rights and responsibilities.
  - Contingency plans for service recovery, data backup and record protection provisions.
  - Service's backup arrangements
  - Service's disaster recovery/contingency plan.
  - Access, ownership, and control of customer data and other confidential information.
  - Availability of financial information (preferably annually).
  - Training.
  - Reasonable penalty and cancellation provisions.
  - Prohibition against assignment of contract by either party without the other's consent.
  - Security precautions on the part of the service provider.
17. If the bank obtains software products from a vendor, ascertain if the vendor supplies source code or maintains a third-party escrow for the benefit of the serviced bank. If documentation and source code are held under Escrow Agreement, the agreement should include the following provisions:
- Conditions whereupon the bank can obtain the source programs and documentation.
  - The media in which the source programs will be released.

Arrangements for auditing the escrow arrangement: An assurance that the most current versions of source programs and documentation will be held by the escrow agent. (Obtain a third-party letter regarding this assurance on a regular basis.)

### **3.7 Accounting and Processing**

1. Determine if the bank's periodic reconciliation procedures incorporate the full scope of transactional capabilities. Determine if the procedures apply to the general ledger and subsidiary accounts, as appropriate.

2. Ensure all general ledger accounts related to Internet banking are reconciled on a timely basis.
  - a) Supervisory personnel should regularly review reconcilements and exception items.
  - b) Ascertain if reconciling items are adequately controlled.
  - c) Procedures for balancing should be well documented and monitored for adherence.
3. Review all suspense accounts related to Internet Banking. Ensure all entries are valid. Trace large items to ascertain how they cleared.
4. Determine if procedures are in place to control customer transfers of uncollected funds from each access point.
5. Confirm that safeguards are in place to detect and prevent duplicate transactions within each system.
6. For systems that permit access to credit lines, determine if draws or credit extensions are adequately controlled.
7. Determine if appropriate audit trails are incorporated into each system.
8. Determine if the Daily Task Log is being completed daily and if a supervisor is reviewing it.
9. Ascertain if the following S1 reports are being reviewed daily by two employees for unusual or large items.
  - Summary Report
  - Manual To Do Report
  - Fast-Pay Report
  - ACH Report
  - Federal ACH Report
  - Bill Payment Report
  - Notifications Report
10. Review customer comments, questions, and complaints logged since last audit. Ensure they were logged on the Customer Service Log and were handled timely.
11. On a sample basis, determine if the following were obtained for new deposit accounts opened through the Internet banking system:
  - a) A credit check approved by an officer of the bank.
  - b) A review to determine if the account satisfied the bank's "Know-Your-Customer Policy."
  - c) If the account is foreign, a review of the Office of Foreign Assets Control list of specially designated persons.

- d) Signed new account application or signature card.
  - e) A properly completed Internet Banking Account Services form (retail customers only).
12. On a sample basis, determine if the following were obtained for new certificate of deposit accounts opened through the Internet Banking system:
- a) A signed new CD account application or CD signature card.
  - b) A review to determine if the account satisfied the bank's "Know-Your-Customer Policy."
  - c) If the account is foreign, a review of the Office of Foreign Assets Control list of specially designated entities.
  - d) Evidence that CD disclosures were mailed or faxed to customers.
13. On a sample basis, determine if the following were obtained for new loan accounts opened through the Internet Banking system:
- a) Ensure no loan applications outside of the bank's normal trade area were approved to commercial customers.
  - b) A signed residential consumer loan application.
  - c) A signed note agreement.
  - d) Evidence that loan disclosures were mailed or faxed to customers.
14. Ascertain if annual financial statements have been received and reviewed for vendors that perform any major services related to Internet Banking Policy. FFIEC
15. Obtain SAS 70 reports on all vendors that process ABTC customer information and perform the following steps:
- a) Ensure that management has identified all third parties related to Internet banking that process information for ABTC.
  - b) Review the findings in the SAS 70s and the management action plans. Ascertain if management has implemented the user controls that each SAS 70 recommends, if applicable.
  - c) Ascertain if management obtains a SAS 70 report from the vendors annually.
  - d) Ensure the period reviewed by the SAS 70s is six months or longer (up to a year).
16. Ensure agreements /contracts are in effect for all Internet banking customers.
- a) The agreement should set forth the rights, responsibilities, and liability for each party.

- b) Determine if the documents address the bank's authority to monitor, store, and retrieve electronic transmissions (including messages and data) between the bank and its customers.
- 17. Determine that written contingency and business resumption plans have been developed for failure of the Internet Banking system and/or communication lines. FFIEC
- 18. Determine whether the bank has an adequate process in place for Internet banking recovery including whether:
  - Internet banking contingency and business resumption plans are reviewed and updated regularly.
  - Specific personnel and staff are responsible for initiating and managing Internet banking recovery plans.
  - The plan ensures that single points of failure for critical network points are adequately addressed.
  - The plan establishes strategies to recover hardware, software, communication links, and data files.
  - Adequate back up agreements and contracts are in place for external vendors or critical suppliers and if these backup arrangements are tested fully.
  - The response process assures that senior management and the Board of Directors are made aware of adverse events as dictated by the severity of damage and monetary loss.
  - Procedures are in place to bring security breaches to the attention of appropriate management and external entities (e.g., CERT, FBI, OCC, etc.)
- 19. Ascertain if contingency and business resumption plans are tested on a regular basis. Ensure management:
  - Requires annual testing of recovery processes and systems.
  - Addresses adverse test results in a timely manner.
  - Informs the board or executive management of test results.
- 20. Review the backup policy. Determine the following:
  - a) A policy exists that defines adequate backup frequency and retention periods for backup data.
  - b) The procedures relating to in-house and off-site storage of backup data and programs are adequate. Ensure critical backups are stored in a secure, off-site location. (Per policy, a backup will be made of the Internet Banking system configuration files and customer configuration files daily. These files will be taken off-site.) (FFIEC) A test of the Internet banking stem backup files is made on an annual basis.

21. Obtain a list of tapes, documentation, etc. that are to be stored off-site and verify their existence.

### **3.8 Legal and Regulatory Matters**

1. Review the website to ensure information regarding the following is accurate:
  - a) Security features
  - b) Customer service access and hours
  - c) Obtaining CRA information
  - d) Names of officers/employees
  - e) Branch locations and operating times
2. Determine if appropriate procedures exist to ensure compliance with Financial Record Keeping and Bank Secrecy Act requirements, including Know Your Customer guidelines. (Procedures should be established to identify potential money laundering activities.)
3. Review the website screens pertaining to deposit accounts for compliance with the following:
  - a) FDIC notice appropriately displayed. (Uninsured products or services clearly designated.) (12 CFR 328)
  - c) Truth in Savings disclosures
  - d) Accuracy of APY and rates offered
  - e) Electronic Funds Transfer Act disclosures
  - f) Expedited Funds Availability Act disclosures
  - g) Reg. D disclosures
4. Review the website screens pertaining to loans for compliance with the following:
  - a) Fair Housing Act signage
  - b) Truth in lending disclosures
  - c) Accuracy of APR and rates offered
  - d) Equal Credit Opportunity disclosures regarding credit denials
  - e) Consumer Leasing Act regarding terms on offered leases
5. Determine whether Office of Foreign Asset Control (OFAC) identification and reporting capabilities are maintained for Internet banking products and services.
6. Determine whether management has established a warning banner for users, announcing that intruders are accessing a private computer and that unauthorised access or use is not permitted and constitutes a crime punishable by law.

7. If the bank is aware of computer-related crimes, determine whether a suspicious activity report (SAR) was filed.

### **3.9 Conclusion Procedures**

1. Prepare Records of Audit Findings (RAFs) listing weaknesses, deficiencies, violations, and other problems noted.
2. Discuss audit findings and recommendations with management.
3. Prepare audit report.

These steps are performed by Internal audit in between external auditor's examinations. External auditors also review these areas. Note: The following sections are to be addressed by external auditors during their examination: Policy, Vendor Management, Passwords, Firewalls, Physical Security, Encryption, Virus Detection and Prevention, Business Resumption and Contingency Planning, Digital Signatures and Certificate Authorities, Monitoring, Internet Service Providers, etc.

### **3.10 Policies and Procedures**

1. Determine whether Internet banking security policies include:
  - a) Clear lines of responsibility for system security - Review the duties of the security administrator. Determine if their authority is adequate to dictate controls and enforce policies.
  - b) Network and data access control.
2. Determine whether Internet banking firewall policies address:
  - Responsibility for firewall maintenance and monitoring
  - Well-defined access rules
  - Access rules that dictate what traffic is allowed or forbidden.
3. Determine whether encryption is adequately addressed in the security policy and the policy includes:
  - Who is responsible for control of encryption processes.
  - How encryption is used.
  - Data classification techniques.
  - Use of encryption to protect transmission of passwords, messages, or data during internal and open network communications sessions.
4. Determine whether policies establish the use of virus detection software and note the products used.



5. Identify whether security policies are periodically reviewed and updated and note whether the board of directors or senior management committee approves the policies.

#### **4.0 CONCLUSION**

The following audit guideline goes a long way to minimise the incidents of fraud in electronic Internet banking. However, the success of the guidelines rests on the faithfulness and sincerity with which the staff of the banks follows the procedures. Though the procedure seems rigorous, is worth all the trouble when we consider the losses associated with e-banking fraud.

#### **5.0 SUMMARY**

- Guidelines for electronic Internet banking are sets of rules, codes and procedures that must formally be adhered to in the course to executing electronic banking process.
- Obtain a current list of the personnel who work in the Internet Banking Department, including their duties.
- Review the prior audit report and note items to be followed up during the current audit.
- Obtain a description and/or diagram of the Internet banking system and its capabilities. Consider hardware, software, points of connectivity to internal systems, and remote access points.
- Determine whether the board, or an appropriate committee, approved the Internet banking system based on a written strategic plan and risk analysis.
- Determine whether the bank has established policies over hypertext links
- Determine whether Internet banking security policies include clear lines of responsibility for system security-Review the duties of the security administrator. Determine if their authority is adequate to dictate controls and enforce policies.
- Ascertain if an Internet banking security officer has been named, as well as a backup.
- On a sample basis, ascertain if users of the Internet banking system have unique user IDs and passwords. Ensure passwords are changed quarterly
- Determine if the bank's periodic reconciliation procedures incorporate the full scope of transactional capabilities. Determine if the procedures apply to the general ledger and subsidiary accounts, as appropriate.

- Review customer comments, questions, and complaints logged since last audit. Ensure they were logged on the Customer Service Log and were handled timely.
- Ascertain if annual financial statements have been received and reviewed for vendors that perform any major services related to Internet banking.
- Ascertain if contingency and business resumption plans are tested on a regular basis. Ensure management
- Determine whether management has established a warning banner for users, announcing that intruders are accessing a private computer and that unauthorised access or use is not permitted and constitutes a crime punishable by law.

## 6.0 TUTOR -MARKED ASSIGNMENT

1. What are the preliminary procedures in obtaining Internet audit documentation?
2. What types of information need to be accurate on a website in the course of a legal and regulatory proceeding of Internet banking system audit.

## 7.0 REFERENCES/FURTHER READINGS

FDIC, June 1998, *Electronic Banking Safety and Soundness Examination Procedures* FFIEC IS Examination Handbook, 1996 (“FFIEC”) Internet Banking.

*Comptroller's Handbook*, October 1999.

Internet Banking Policy, National Bank of Commerce, September 2000 (“P”) Last revised December 2001.

## MODULE 3

Unit 1	Risks and Security in Electronic Banking
Unit 2	Introduction to Biometrics
Unit 3	Application of Biometrics and Artificial Intelligence (AI) In Electronic Fraud Detection
Unit 4	Identifying and Responding to Electronic Fraud Risks: <i>The Case of Australia</i>

## **UNIT 1     RISKS AND SECURITY IN ELECTRONIC BANKING**

### **CONTENTS**

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
  - 3.1 Risks of Insecurity
    - 3.1.1 IT Environment Risks
    - 3.1.2 IT Operations Risk
    - 3.1.3 IT Product/Services Risks
  - 3.2 Dealing with Insecurity
  - 3.3 How to Confirm that an Online Bank is Legitimate and that Your Deposits are Insured
    - 3.3.1 Read Key Information about the Bank Posted on Its Website
    - 3.3.2 Protect Yourself from Fraudulent Websites
    - 3.3.3 Verify the Bank's Insurance Status
    - 3.3.4 For Insurance Purposes, Be Aware that a Bank May Use Different Names For Its Online and Traditional Services; This Does Not Mean You Are Dealing with Separate Banks
    - 3.3.5 Know Where to Get More Information about FDIC Insurance
  - 3.4 How to Protect Your Privacy
  - 3.5 How to Help Keep Your Transaction Secure
  - 3.6 Policies
  - 3.7 Network Protection and Firewalls
    - 3.7.1 Firewalls at Fidelity Investment
  - 3.8 Network Information Security Issues
  - 3.9 Security Techniques
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

### **1.0 INTRODUCTION**

Bankers by their very nature are focused on security. This is natural because in the ultimate analysis they are dealing with other people's funds and it is a matter of trust. The risk of fraud and cheating is always there. When we talk of security in the computerised and electronic banking environment, we have to take note of the new type of risks that arise because of the computerised banking environment.

### **2.0 OBJECTIVES**

At the end of this unit you should be able to:

- explain types of risks associated with computerised electronic banking system
- identify areas in which computerisation in electronic banking can lead to detection and prevention of fraud
- explain how to determine if electronic banking is legitimate and safe for a banking transaction
- answer the questions on how to establish privacy and secure transactions in online electronic banking
- explain protective security measures to secure an e-banking network.

### 3.0 MAIN CONTENT

#### 3.1 Risks of Insecurity

There are risks associated with computer and telecommunication systems (RBI, February 1998) “, the risks are under three heads:

- Environment risks
- IT operations risks
- IT product risks.

##### 3.1.1 IT Environment Risks

This category represents the inherent risks that arise due to the commercial and business environment within which the computer and telecommunication systems are operating. They are described briefly below:

- **Regulatory Risk** - Banks must operate within a set regulatory framework. The design and operation of a bank's computer systems must reflect and comply with the regulatory framework in place. The greater the extent of computerisation at a bank, the greater the possibility that change in banking regulations will affect computer systems. Regulatory breaches can result in diminished reputation, increased cost of capital, limited business opportunities and ultimately loss of a banking license. The lack of a legal framework covering electronic transactions can increase the likelihood of disputes arising relating to such transactions.
- **Strategic Risk** - Strategic planning in a bank sets out corporate or departmental objectives, which help to ensure an effective and

efficient organisation now and in the future. The IT department particularly requires strategic objectives, for without them, IT management may not be able to produce an effective IT strategy and deliver IT to meet the business' needs. If a bank is without an IT strategy, the user management's requirements may not be adequately communicated to IT Management. As a result the bank's IT resources may not be deployed appropriately to meet its overall business strategy.

When a bank adopts inappropriate IT strategies, this may place undue pressure on the bank's IT resources and systems to adapt to new business environments as new products and services come on line. A risk exists that short term fixes may be made to the detriment of longer term objectives and projects. In addition, business pressures may result in system changes being implemented too quickly and before they have been adequately tested.

The failure of IT strategies to take into account the changing needs of the bank may lead to the current systems becoming obsolete over time, with competitors gaining a competitive advantage through the utilisation of new more advanced and cost effective technologies ahead of the bank concerned.

- **Organisation Risk** - The organisational structure of a bank can determine the effectiveness of the bank's use of IT. Where the organisational structure fails to provide and define reporting lines and responsibilities for the IT functions, this can lead to misunderstandings of responsibility and a poor distribution of human and financial resources. In addition, poor segregation of duties can increase the risk of error and fraud within a computer and telecommunication environment.
- **Location Risk** - As banks become computerised, they depend increasingly upon their technology resources to achieve the business objectives. The technology resources are susceptible to the risks of unforeseen and sometimes naturally occurring events. Depending on the location of a bank's data processing equipment, it can be susceptible to natural event such as floods and earthquakes or storms and other events such as riots or sabotage.
- **Outsourcing Risk** - It is increasingly common for banks to outsource some or all of their data processing and IT. While all the other types of risk still need to be addressed, when outsourcing takes place, there are some additional risks, which need to be considered. Without proper management control and documentation, the responsibilities and liabilities of supplier and customer may not be

clear. Over reliance on a single supplier increases the risks from supplier failure and may lead to unacceptably high costs.

### 3.1.2 IT Operations Risk

Operations risk relates to those risks arising from day to day transaction processing on computer systems. The various components of IT operations risk can be classified under the following headings:

- **Error Risk** - Errors in a computerised environment may arise from a number of sources including errors made during the development and amendment of computer programs, simple errors in data entry by terminal operators, and misuse of system housekeeping tools and sensitive facilities. These errors may affect the completeness and accuracy of transactions, balances and management information.

Bank computer programs are often highly complex, containing typically thousands of lines of computer coding any number of which may contain errors. Whilst these programs may have been well tested, a risk still exists that errors can remain inactive and dormant for a number of years, only to appear when a certain set of circumstances occurs. Standard software packages are also not immune from the introduction of errors. These may occur when the packages are "customised" by the vendor and adapted to the particular bank.

- **Computer Fraud Risk** - A computerised environment provides a number of new opportunities for fraudsters. This is primarily due to the ease with which the fraudsters can hide their actions on computer systems and the speed with which fraudulent activity can take place. Most banking systems contain control facilities and produce reports designed to assist in the prevention or detection of fraud. These too however may be highly vulnerable to personnel with powerful privileges who can manipulate access to computer terminals or files.

It is imperative that a bank is aware of the vulnerable points within its system and guards against new opportunities for fraud, which may materialise, especially during times of business and systems change. Particular risks are also associated with the implementation of new systems and all the security requirements of a new system should be considered prior to a system being specified or designed. If this exercise does not take place, the bank is at risk of the new systems being unreliable and difficult to secure against unauthorised access or activity.

- **Disclosure Risk** - Information held on a bank's computer and passed around its computer network includes very sensitive financial and other data about the bank's customers. Accidental or intentional

disclosure of this information can have a negative reputation impact on a bank, increasing the risk of fraud against its customers of leaving the bank open to legal charges.

- **Interruption Risk** - As banks become increasingly computerised, their ability to be able to operate for any significant length of time without their computer and telecommunications systems fall. The bank is ultimately reliant upon a number of different components which together make up the bank's technical infrastructure any one of which may bring the system down in the event of an unexpected or planned event occurring.

The impact of a discontinuity of computer operations can be dramatic. Processing backlogs may build up which can take hours or even days to process and where ATMs are being used, the impact on the customer will be almost immediate. If computer facilities and related infrastructures are not adequately protected and secured, the result may be a major impact upon the continuity and even going concern of banking operations. Inadequate continuity arrangements may result in a loss of business, damaged reputations and loss of assets.

### 3.1.3 IT Product/Services Risks

Banks may implement technology-based products to improve operational efficiency and effectiveness. Whilst the operational risks associated with these products remain fundamentally unchanged, the way in which management's design and implement a control framework to mitigate against those risks is different. Examples, of areas which may require additional and specific control procedures in place, include the following - (1) Automated teller machines; (2) Money transmissions and settlements; (3) Computer based dealing activities; (4) Derivatives trading.

## 3.2 Dealing with Insecurity

The question before us now is how do we tackle the issue of security? The first point for consideration is that in the era of computerised banking environment, if we are not effectively computerised, we are going to be losing heavily. The linkage between computerisation and checking frauds in the banking system would be obvious.

As regards the question whether computerisation would help banks in prevention and early detection of frauds, frauds can be broadly classified as (a) frauds in non-credit areas and (b) frauds in credit areas. In non-credit areas mainly frauds relate to fraudulent encashment of cheques, withdrawal slips, refund orders, demand drafts, bankers cheques,

misappropriation as also fraudulent transactions in the books of branches put through by the bank's own staff. Existing computerised system and upgrading thereof will help in prevention as also early detection of frauds which will save bank's precious funds as also will protect the long term interest of bank employees who unwittingly become prey to the design of unscrupulous elements.

Following are the areas where full-fledged computerisation will have effect in prevention and early detection of frauds.

1. Fraudulent encashment of cheques bearing forged signatures occur because the passing officials do not find it convenient to verify the signature stored in signature card cabinets requiring manual location of the signature. If specimen signatures are captured in the computer, it will facilitate easy verification and provide security against tampering.
2. Stop payment instructions received from account holders with regard to lost cheques can be put in computer so that a caution signal would be available whenever a lost cheque is presented for payment.
3. Manipulation of books by unscrupulous staff inter-alia casting of wrong balance and making wrong credit entries can be either prevented or detected promptly because the computerisation would enable tallying / balancing of books on daily basis.
4. The reconciliation of transactions relating to drafts issued and paid through computerised system would help early detection of fraudulent payments.
5. Frauds relating to local clearing operations may be minimised through prompt reconciliation of number and amount of cheques through computerised system.
6. Attempts of unscrupulous staff to perpetrate frauds by raising fake credits through inter branch accounts may be thwarted through computerised system for reconciliation of entries between originating branches and responding branches.
7. By introduction of pass book writing machines frauds relating to misappropriation of cash receipts by cash department staff can be prevented or early detected.
8. There is increasing trend in payment of lost/fake DDs presented by fraudulent means. Computerisation and continuous updating of data related to stolen/lost drafts on the system can help in



reducing this. Officers' signatures captured in the computer can be used to verify whether the DDs are signed by the concerned officers.

9. As per the guidelines of RBI, MICR clearing and Electronic Clearance System have been introduced at metro centres to take care of corporate clients. The Service Branch or the main branch does the work of intermediary between the local branches of the bank and clearing house. Lack of proper reconciliation of number and amount of cheques sent by branches to the service branch / main branch and vice versa on a daily basis has facilitated perpetration of massive fraud. A software system for daily reconciliation, if introduced, can be used to avert or detect such frauds.
10. As regards advances, in credit related frauds, it would help banks if computerised data base of parties enjoying credit facilities from different banks in the same centre is available to avoid double financing, to know the state of affairs of the existing account, and to ensure that the same persons do not enjoy facilities under different names or firms.
11. Database of information of fraudsters, willful defaulters with photographs of the proprietors / partners / directors etc will help the banking system
12. Quick exchange of information relating to transactions in corporate accounts, remittances, clearance of instruments, payment of dividend warrants, interest warrants, refund orders and reconciliation thereof, etc. will enhance customer service and help prevent frauds.

### **3.3 How to Confirm That an Online Bank is Legitimate and that Your Deposits are Insured**

Whether you are selecting a traditional bank or an online bank that has no physical offices, it's wise to make sure that it is legitimate and that your deposits are federally insured. Here are tips specifically designed for consumers considering banking over the Internet.

#### **3.3.1 Read Key Information About the Bank Posted on Its Website**

Most bank websites have an "About Us" section or something similar that describes the institution. You may find a brief history of the bank, the official name and address of the bank's headquarters, and information about its insurance coverage from the FDIC.

### 3.3.2 Protect Yourself From Fraudulent Websites

For example, watch out for copycat websites that deliberately use a name or web address very similar to, but not the same as, that of a real financial institution. The intent is to lure you into clicking onto their website and giving your personal information, such as your account number and password. Always check to see that you have typed the correct web site address for your bank before conducting a transaction.

### 3.3.3 Verify The Bank's Insurance Status

To verify a bank's insurance status, look for the familiar FDIC logo or the words "Member FDIC" or "FDIC Insured" on the website.



Also, you should check the FDIC's online database of FDIC-insured institutions. You can search for an institution by going to **Bank Find** (formerly "Is My Bank Insured?"). Search by name, city, state or zip code of the bank, and click the "Find" button. A positive match will display the official name of the bank, the date it became insured, its insurance certificate number, the main office location for the bank (and branches), its primary government regulator, and other links to detailed information about the bank. If your bank does not appear on this list, contact the FDIC.

Some bank websites provide links directly to the FDIC's website to assist you in identifying or verifying the FDIC insurance protection of their deposits.

Also remember that not all banks operating on the Internet are insured by the FDIC. Many banks that are not FDIC-insured are chartered overseas. If you choose to use a bank chartered overseas, it is important for you to know that the FDIC may not insure your deposits. Check with your bank or the FDIC if you are not certain.

### **3.3.4 For Insurance Purposes, Be Aware that a Bank May Use Different Names for Its Online and Traditional Services; This Does Not Mean You are Dealing with Separate Banks**

This means, for example, that to determine your maximum FDIC insurance coverage, your deposits at the parent bank will be added together with those at the separately named bank Web site and will be insured for up to the maximum amount covered for one bank. Talk to your banker if you have questions.

### **3.3.5 Know Where to Get More Information about FDIC Insurance**

Don't worry about your deposit insurance coverage if you or your family has less than \$100,000 in all your accounts combined at the same FDIC-insured bank. But if your accounts total \$100,000 or more, find out if they're within the insurance limit. Contact your bank for more information.

For additional assistance from the FDIC about the legitimacy of an institution or the insurance of your deposits, call the FDIC's Division of Compliance and Consumer Affairs toll-free at 800-934-3342 or send an e-mail via the FDIC's online Customer Assistance page.

The FDIC's Web site also has an interactive service called EDIE (Electronic Deposit Insurance Estimator) that can help you determine the amount of your insurance coverage. Or, you can read the online deposit insurance brochure "Your Insured Deposits."

It's important to note that only *deposits* offered by FDIC-insured institutions are protected by the FDIC. Non-deposit investment and insurance products, such as mutual funds, stocks, annuities and life insurance policies that may be sold through Web sites or at the bank itself, are *not* FDIC-insured, are not guaranteed by the bank, and may lose value.

## **3.4 How to Protect Your Privacy**

Some consumers may want to know how their personal information is used by their bank and whether it is shared with affiliates of the bank or other parties.

Banks are required to give you a copy of their privacy policy once you become their customer, regardless of whether you are conducting business online or offline. You may also see a copy of it posted at the

bank's website. By reviewing this policy you can learn what information the bank keeps about you, and what information, if any, it shares with other companies.

Banks may want to share information about you to help market products specific to your needs and interests. If you do not wish to participate in information sharing, however, you have the right to prevent your bank from sharing your private personal information with parties not affiliated with the bank, except in certain limited circumstances. Your bank should provide a clear method for you to "opt out" of this type of information sharing.

You may have heard that some companies track your Web browsing habits while at their site, to understand your interests and then to market particular services or promotions. You may want to ask whether your bank tracks your browsing habits if these practices concern you. Also, your Web browser may enable you to block the ability of outside companies to track your browsing habits.

Your bank and your Internet service provider may have more information about how to protect your privacy online.

### 3.5 How to Help Keep Your Transaction Secure

The Internet is a public network. Therefore, it is important to learn how to safeguard your banking information, credit card numbers, Social Security Number and other personal data.

Look at your bank's website for information about its security practices, or contact the bank directly.

Also learn about and take advantage of security features. Some examples are:

- **Encryption** is the process of scrambling private information to prevent unauthorised access. To show that your transmission is encrypted, some browsers display a small icon on your screen that looks like a "lock" or a "key" whenever you conduct secure transactions online. Avoid sending sensitive information, such as account numbers, through unsecured e-mail.
- **Passwords or Personal Identification Numbers (PINs)** should be used when accessing an account online. Your password should be

unique to you and you should change it regularly. Do not use birthdates or other numbers or words that may be easy for others to guess. Always carefully control to whom you give your password. For example, if you use a financial company that requires your password in order to gather your financial data from various sources, make sure you learn about the company's privacy and security practices.

- **General security** over your personal computer such as virus protection and physical access controls should be used and updated regularly. Contact your hardware and software suppliers or Internet service provider to ensure you have the latest in security updates.

If you have a security concern about your online accounts, contact your bank to discuss possible problems and remedies.

### **3.6 Policies**

Policies serve to set the tone for how security is viewed within an organisation. Useful security policies have widespread management support and are detailed to give an organisation a clear sense of direction. Good policies also include guidelines for implementing disaster recovery plans, designing security controls into applications, establishing system-user access capabilities, carrying investigations of computer crimes, and disciplining employees for security breaches.

In creating information security policies, it is critical that policies are well matched to the corporate culture. Consciously or unconsciously, employees will resist policies that conflict with the corporate ways of doing things. Moreover, policies that conflict with basic, underlying beliefs, attitudes and values of the organisation are likewise unlikely to be effective. Ultimately, mismatches result in policies that are either completely ignored or sub optimal in their impact.

### **3.7 Network Protection and Firewalls**

#### **3.7.1 Firewalls At Fidelity Investment**

Fidelity Investments, the largest U.S. mutual fund company and active broker, allows its customers and prospective customers to personalise their access to information available on Fidelity's website, including their own account access and transactional information. This service called Web express, was pioneered by Fidelity and includes information about balances, and stock positions, historical transactions, online registration for new accounts, secure log-ins, real-time quote on equities, mutual funds, options, and indices, and trading capabilities. A major

concern is the protection of security and privacy, a difficult task since even simple transactions, require complex operations, including dynamically generated HTML.

#### Protecting Against Viruses

Possible Entrance of Viruses	Countermeasure
Viruses pass through firewall undetected (from the Internet)	User must screen all downloaded programs and documents before use
Virus resident on networked server; all users at risk	Run virus scan, daily, comprehensive backup to restore data; audit trail
Infected floppy; local servers system at risk; files shared or put on server can spread virus	Virus checker to screen floppies locally
Mobile or remote users exchange or update large amounts of data, risk of infection is greater.	Scan files before upload or after download; make frequent backups.

### 3.8 Network Information Security Issues

Inadequate security is thought to be the main hindrance to the Internet becoming a veritable market place. Network information security has four main issues:

- **Access Control and Authorisation:** This area of security deals with the question of who is allowed into a network, and for what purpose. However, the interdependence of authorisation process among networks and among host node complicates control and authorisation.
- **Information Authenticity:** This area deals with identifying the source of information i.e. the originator of the message. When an organisation's network is connected to many others, it is impossible to identify network user with the traditional login and location method used in mainframes. Eavesdroppers can copy these and impersonate legitimate users. One of the proposed methods of overcoming this problem is the use of digital signatures.
- **Information Integrity:** Ensuring the integrity of information means ensuring that the data has not been altered. When information enters the organisation's network from other networks, it is much harder to

ensure that information has been lost. Special protocols have been designed for this purpose.

- **Information Privacy:** Privacy in networks generally means that personal and confidential information is not subject to eavesdropping. Cryptography or cryptosystems often achieves privacy.

### 3.9 Security Techniques

The effectiveness of security techniques depends upon the deterrent effect of having the administrative policies in place, management commitment to good security and user security awareness. To prevent losses from insecure systems, security software can also be used. Methods to detect abuse activities involve monitoring system use, suspicious systems activity, and security violation. Through use of this kind of methods, management delivers the message that security is important to the firm and that there are penalties for violating security.

Methods that deal with specific aspects of security include:

- **Physical Security:** These methods are primarily aimed at protecting system users from theft. They include locks, alarms, and embedding the company logo on the hardware. In addition restricted entrance to sensitive departments is often used and combined with automatically monitored entrances and departure recordings. Other useful measures include administrative regulations ensuring that removable disks with secured data be locked up and that sensitive data be kept only on secured disk.
- **Backup:** Disks and tape backups are used to deal with data loss due to faulty devices and human errors. It is often suggested that companies utilise backups to ensure their chances of survival in the event of data loss.
- **Redundancy:** Redundant data, input-output devices, and processors can be used as a method of fault management in crucial network management system. These mechanisms provide fault-free operations by detecting, isolating, and resolving faults. Built-in redundancy methods often use expert systems.
- **Passwords:** The first line of defense in maintaining data security is enforcing a sign-in and password verification procedure (login). This procedure can be augmented by administrative policies that require that power be turned off when PC is not in active use. An extended defense can be achieved by using available security software that

force a login and automatically encrypts protected subdirectories so that, if the login is bypassed, the files are not available.

- **Authorising Access:** Once a user has entered a system using a password, many database systems come with an in-built authorisation mechanism that enable the system administrators to authorise different types and location of access to data according to user identification or group. Authorisation control and security policy enforcement are also available as standalone software security tools.
- **Encryption:** Even when a user has access to certain data, encryption can be used to ensure that the authorisation process in a database management system or a network is not circumvented. This method is often used to secure data and communications. There are two types of cryptographic methods: those applying common keys and those applying private keys. The common key methods apply the same key for encryption and decryption. These methods are often faster and are often used for bulk data. A method frequently used in this situation is the Digital Encryption Standard (DES) algorithm. The private key method allocates two keys to each user: a public key for encrypting and a private key for decrypting. One of the commonly used algorithms for this type is RSA. Encryption algorithms are mostly only computationally secure, i.e. breaking the code is possible, but requires an unfeasible amount of computational time and resources.
- **Firewalls.** Firewalls are computerised barrier that controls and prevents illicit messages and users from entering a network or part of it. This feature is essential when companies allow their customers and suppliers enter access their internal network. Firewall protects resources by securing servers and sites as well as transactions. This is done by controlling authentication, message integrity and unauthorised listening. The two currently available methods are *channel-based security* and *document-based security*. A channel-based security standard such as SSL (secure socket layer), secures the entire channel, while a document-based standard such as SHTTP (secure hypertext transport protocol) only guarantees that specific document broadcast will be secure. The world-wide web commerce already existed for users with SSL servers.

The most common types of firewall are:

- i. **Router-Based Filter:** These control the traffic at the IP (Internet Protocol) level of TCP/IP (Transmission Control Protocol) by



controlling the packets allowed into the network. This method is probably the most commonly used at present. However, it does not work well non-packet protocols.

- ii. **Gateways:** These firewalls reside on the host computers and use the host computer to log activities via security software.
- iii. **Isolated Networks.** This method is similar to gateways, with the exception that it creates an isolated internal network that connects to the outside network through a gateway.
- iv. **Electronic Signatures:** The digital signature algorithm (DSA) is a digital signature and verification mechanism used for digital rather than written signatures. DSA enables verification of signature, message origin, and message integrity without giving away information that would make signature forgery possible. DSA achieves this by allotting two different digital keys to each signature bearer: a secret private key for encrypting the message and a public key for decrypting. Only the signature bearer knows the private key, while all the network users know the public key

#### 4.0 CONCLUSION

Safety and security have remained a major concern in the successful deployment of technology in modern-day electronic banking transactions. Continually, several security and safety measures are being developed to counter fraudulent schemes and prevent hackers from having access to e-banking networks. No singular measure is a full proof, but a collection of compatible measures have been found to be highly effective in minimising fraudulent threats and attacks.

#### 5.0 SUMMARY

- Bankers by their very nature are focused on security. This is natural because in the ultimate analysis they are dealing with other people's funds and it is a matter of trust.
- There are risks associated with computer and telecommunication systems
- Banks must operate within a set regulatory framework. The design and operation of a bank's computer systems must reflect and comply with the regulatory framework in place.
- It is increasingly common for banks to outsource some or all of their data processing and IT. While all the other types of risk still need to be addressed, when outsourcing takes place, there are some additional risks, which need to be considered.

- A computerised environment provides a number of new opportunities for fraudsters.
- Banks may implement technology-based products to improve operational efficiency and effectiveness.
- The question before us now is how do we tackle the issue of security? The first point for consideration is that in the era of computerised banking environment, if we are not effectively computerised, we are going to be losing heavily.
- Whether you are selecting a traditional bank or an online bank that has no physical offices, it's wise to make sure that it is legitimate and that your deposits are federally insured.
- Fraudulent encashment of cheques bearing forged signatures occur because the passing officials do not find it convenient to verify the signature stored in signature card cabinets requiring manual location of the signature. If specimen signatures are captured in the computer, it will facilitate easy verification and provide security against tampering
- Also, you should check the FDIC's online database of FDIC-insured institutions. You can search for an institution by going to **Bank Find** (formerly "Is My Bank Insured?").
- Some consumers may want to know how their personal information is used by their bank and whether it is shared with affiliates of the bank or other parties.
- The Internet is a public network. Therefore, it is important to learn how to safeguard your banking information, credit card numbers, Social Security Number and other personal data.
- Policies serve to set the tone for how security is viewed within an organization. Useful security policies have widespread management support and are detailed to give an organisation a clear sense of direction.
- Fidelity Investments, the largest U.S. mutual fund and active broker, allow its customers and prospective customers to personalise their access to information available on Fidelity's website, including their own account access and transactional information.
- Inadequate security is thought to be the main hindrance to the Internet becoming a veritable market place.
- The effectiveness of security techniques depends upon the deterrent effect of having the administrative policies in place, management commitment to good security and user security awareness.
- The first line of defense in maintaining data security is enforcing a sign-in and password verification procedure (login). This procedure can be augmented by administrative policies that require that power be turned off when PC is not in active use.

Firewalls are computerised barriers that control and prevent illicit messages and users from entering a network or part of it. This feature is

essential when companies allow their customers and suppliers access their internal network.

## **6.0 TUTOR - MARKED ASSIGNMENT**

1. Discuss some information technology risks encountered in electronic banking.
2. Mention 5 specific techniques needed to ensure the safety of a network transaction.

## **7.0 REFERENCES/FURTHER READINGS**

Anderson, R.G (1994). *Data Processing: Principles & Practice*, Vol. 1. Pitman Publishing.


Anderson, R.G, (1994). *Data Processing: Information Systems & Technology*, Vol. 2, Pitman Publishing.

Turban, E., McLean, E. & Wetherbe, J. (1999). *Information Technology Management*. Juan Wiley & Sons Inc.

Vittal, N. "Security, Controls and Audit in Computerized Banking Environment". NIBSCOM Seminar on 09.03.2000. New Delhi.

## UNIT 2 INTRODUCTION TO BIOMETRICS

### CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
  -  3.1 Why Biometrics?
  - 3.2 Classification of Some Biometric Traits
  - 3.3 Functions of Biometrics
  - 3.4 Forms of Biometrics
    - 3.4.1 Handwritten Signatures
    - 3.4.2 Face Recognition
    - 3.4.3 Fingerprints
    - 3.4.4 Voice Recognition
    - 3.4.5 Other Systems
  - 3.5 Performance Measurement
  - 3.6 Issues and Concerns
  - 3.7 Sociological Concerns
  - 3.8 Danger to Owners of Secured Items
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

### 1.0 INTRODUCTION

**Biometrics** (ancient Greek: *bios* = "life", *metron* = "measure") is the study of methods for uniquely recognising humans based upon one or more intrinsic physical or behavioral traits

Biometrics identifies people by measuring some aspects of individual anatomy or physiology (such as your hand geometry or fingerprint), some deeply ingrained skill, or other behavioral characteristic (such as your handwritten signature), or something that is a combination of the two (such as your voice). Over the last quarter century or so, people have developed a large number of biometric devices; this rapidly growing market is now worth about \$50 million a year. The use of hand geometry was used to identify staff at a nuclear reactor in the late 1970s. But the best established biometric techniques predate the computer age.

Some researchers have coined the term **behaviometrics** for behavioral biometrics such as typing rhythm or mouse gestures where the analysis can be done continuously without interrupting or interfering with user activities.

## 2.0 OBJECTIVES

At the end of this unit, you should be able to:

- explain what biometrics is and why biometrics is deployed in fraud detection and prevention schemes
- classify and characterise biometrics
- identify the functions and applications of biometric in fraud detection
- identify the forms of biometrics that exist
- explain the process of measuring the performance of biometrics
- explain the issues and challenges facing biometrics and its applications in fraud prevention and detection.

## 3.0 MAIN CONTENT

### 3.1 Why Biometrics?

The modern rapid advancements in networking, communication and mobility increased the need of reliable ways to verify the identity of any person. Nowadays identity verification is mainly performed in two ways:

- **Possession-Based:** The whole security is based on a "token" the user has (such as a credit card or a document). If it is lost, somebody else might use it to falsify his identity.
- **Knowledge-Based:** Using a password. Even if we use the best encrypting algorithm, the whole security is based on the key. If it is too short, it is simple to guess it or crack it making several attempts, but if it is too complicated it can't be remembered and the common user will keep it written somewhere, so it can be lost or stolen

Those weaknesses of standard validation systems can be avoided if our own body becomes our key. Particular characteristics of the body or habits are much more complicated to forge than a string of text, even if it is very long. Reliability of biometric systems will be discussed later, but it is evident that using biometrics adds a complexity to identification systems that would be hard to reach with a standard password-based approach. The main advantages of biometrics over a standard system are:

- biometric traits cannot be forgotten or mislaid, and can be lost only through trauma (whereas passwords can be forgotten and tokens easily lost or mislaid).
- biometric traits are relatively difficult to copy, share and distribute (passwords can be announced in crackers' websites).

- *pace* the previous point, biometric traits require the person being authenticated to be present at the time and point of authentication.

Moreover biometric systems can be used in conjunction with passwords or tokens, thus improving the security of existing systems without replacing them.

### 3.2 Classification of Some Biometric Traits

Biometric characteristics can be divided in two main classes:

- **Physiological** traits which are related to the shape of the body. The oldest traits, used for more than 100 years, are fingerprints. Other examples are face recognition, hand geometry and iris recognition.
- **Behavioral** traits which are related to the behavior of a person. The first characteristic to be used, still widely used today, is the signature. More modern approaches are the study of keystroke dynamics and of voice.

Strictly speaking, *voice* is also a physiological trait because every person has a different pitch, but voice recognition is mainly based on the study of the way a person speaks, which is why it is commonly classified as behavioral.

There are many other biometric strategies being developed such as those based on gait (way of walking), retina, hand veins, ear recognition, facial thermogram, DNA, odor and palm prints.

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters:

- **Universality** describes how commonly a biometric is found in each individual.
- **Uniqueness** is how well the biometric separates one individual from another.
- **Permanence** measures how well a biometric resists aging.
- **Collectability** explains how easy it is to acquire a biometric for measurement.
- **Performance** indicates the accuracy, speed, and robustness of the system capturing the biometric.
- **Acceptability** indicates the degree of approval of a technology by the public in everyday life.
- **Circumvention** is how hard it is to fool the authentication system.

The following table shows a comparison of existing biometric systems in terms of these parameters:

**Table 1**

Comparison of various biometric technologies, according to A. K. Jain <sup>[2]</sup> (H=High, M=Medium, L=Low)							
Biometrics:	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
<a href="#">Face</a>	H	L	M	H	L	H	L
<a href="#">Fingerprint</a>	M	H	H	M	H	M	H
<a href="#">Hand geometry</a>	M	M	M	H	M	M	M
<a href="#">Keystrokes</a>	L	L	L	M	L	M	M
<a href="#">Hand veins</a>	M	M	M	M	M	M	H
<a href="#">Iris</a>	H	H	H	M	H	L	H
<a href="#">Retinal scan</a>	H	H	M	L	H	L	H
<a href="#">Signature</a>	L	L	L	H	L	H	L
<a href="#">Voice</a>	M	L	L	M	L	H	L
<a href="#">facial thermogram</a>	H	H	L	H	M	H	H
<a href="#">Odor</a>	H	H	H	L	L	M	L
<a href="#">DNA</a>	H	H	H	L	H	L	L
<a href="#">Gait</a>	M	L	L	H	L	H	M
<a href="#">Ear recognition</a>	M	M	H	M	M	H	M

A. K. Jain ranks each biometric system as being low, medium, or high. A low ranking one indicates poor performance in the evaluation criterion whereas a high ranking one indicates a very good performance.

### 3.2 Functions of Biometrics

A biometric system can provide the following two functions:

- **Verification:** *Is he the person he claims to be?* Somebody claims to be a person whose biometric info is already known (e.g. it was stored on a card or in a database). We want to extract new biometric info from the person and check if those are matching with the ones we have. This way we can verify the identity of a person. In other words, it's a 1:1 match verification.
- **Identification:** *Who is he?* We extract biometric information from a person and we compare them with a database. It is a much more difficult task than verification because we have to compare that information with all people in the database.

These applications are of immense benefit to electronic banking and can assist in fraud detection.

### 3.4 Forms of Biometrics

#### 3.4.1 Handwritten Signatures

Handwritten signatures had been used in classical China, but carved personal seals were considered to be higher status, and are still used for

serious transactions in China, Japan, and Korea to this day. Europe was the other way around: seals had been used in medieval times, but as writing spread after the Renaissance, people increasingly just wrote their names to signify assent to business and other documents. Over time, the signature became accepted as the standard way of doing this in the West. Every day, billions of dollars' worth of contracts even in electronic banking transactions are concluded by handwritten signatures on documents, and how these can be replaced by electronic signatures is a hot policy and technology issue.

### **How Secure are Handwritten Signatures?**

The probability that a forged signature will be accepted as genuine mainly depends on the amount of care taken when examining it. Many bank card transactions in stores are accepted without even a glance at the specimen signature on the card—so much so that many Americans do not even bother to sign their credit cards. (This can cause problems when traveling in more punctilious countries such as Germany or Switzerland.) But even diligent signature checking doesn't reduce the risk of fraud to zero. An experiment showed that 105 professional document examiners, who each did 144 pair-wise comparisons, misattributed 6.5% of documents. Meanwhile, a control group of 34 untrained people of the same educational level got it wrong 38.3% of the time, and the nonprofessionals' performance couldn't be improved by giving them monetary incentives. Errors made by professionals are a subject of continuing discussion in the industry, but are thought to reflect the examiner's assumptions and preconceptions. As the participants in these tests were given reasonable handwriting samples rather than just a signature, it seems fair to assume that the results for verifying signatures on checks or credit card vouchers would be significantly worse.

So handwritten signatures are surrounded by a number of conventions and special rules which vary from one country to another. The essence of a signature is the intent of the signer, so an illiterate person's "X" on a document is just as valid as a monarch's flourish. In fact, a plaintext name at the bottom of an email message also has just as much legal force, except where there are specific regulations requiring the transaction to be in writing. There may be thousands of such in each jurisdiction. Meanwhile, it's actually very rare for signatures to be disputed in court cases, as the context generally makes it clear who did what. So we have a very weak biometric mechanism that works quite well in practice—except that it's choked by procedural rules that vary by country and by application.



Sorting out this mess, and imposing reasonably uniform rules for electronic documents, is a subject of much international activity.. For now, note the form of a signature and the ease with which it can be forged, and whether it has legal validity in a given context, are largely independent questions.

There is one application, though, where effective automatic recognition of handwritten signatures could be very valuable. This is check clearing. In a bank's check processing center, it is typical practice that you only verify signatures on checks over a certain amount—perhaps \$1,000, perhaps \$10,000, perhaps a percentage of the last three months' movement on the account. The signature verification is done by an operator who sees, simultaneously presented on-screen, the check image and the customer's reference signature.

Verifying checks for small amounts is not economic unless it can be automated, so a number of researchers have worked on systems to compare handwritten signatures automatically. This turns out to be a very difficult image-processing task because of the variability between one genuine signature and another. A much easier option is to use a *signature tablet*. This is a sensor surface on which the user does a signature; it records not just the shape of the curve but also its dynamics (the velocity of the hand, where the pen was lifted off the paper, and so on). Tablets are used to identify users in some high-value applications, including securities dealing.

Like alarm systems, most biometric systems have a trade-off between false accept and false reject rates, often referred to in the banking industry as the *fraud* and *insult* rates, and in the biometric literature as *type 1* and *type 2* errors. Many systems can be tuned to favor one over the other. The *equal error rate* is when the system is tuned so that the probabilities of false accept and false reject are equal. For common signature recognition systems, the equal error rate is about 1%. This is not fatal in an operation such as a bank dealing room. If one of the dealers tries to log on one morning and his PC rejects his signature, he can just try again. If there is a persistent failure, he can call the system administrator and have the machine reset. However, it is a show-stopper in a retail store. If one transaction in a hundred fails, the aggravation to customers would be unacceptable. So U.K. banks set a target for biometric of a fraud rate of 1% and an insult rate of 0.01%, which is beyond the current state of the art in signature verification.

In general, biometric mechanisms tend to be much more robust in attended operations, where they assist a guard rather than replacing him. The false alarm rate may then actually help by keeping the guard alert.

### 3.4.2 Face Recognition

Recognising people by their facial features is the oldest identification mechanism of all, going back at least to our early primate ancestors. Biologists believe that a significant part of our cognitive function evolved to provide efficient ways of recognising other people's facial features and expressions. For example, we are extremely good at detecting whether another person is looking at us or not. In theory, humans' ability to identify people by their faces appears to be very much better than any automatic system produced to date.

The human ability to recognise faces is also important to the security engineer because of the widespread reliance placed on photo IDs. Drivers' licenses, passports, and other kinds of identity card are not only used directly to control entry to computer rooms, but also bootstrap most other systems. The issue of a password, or a smartcard, or the registration of a user for a biometric system using some other technique such as iris recognition, is often the end point of a process which was started by that person presenting photo ID when applying for a job, opening a bank account, or whatever. But even if people are good at recognizing friends in the flesh, how good are they at identifying strangers by photo ID?

The simple answer is that they're not. Psychologists at the University of Westminster conducted a fascinating experiment with the help of a supermarket chain and a bank. They recruited 44 students and issued each of them with four credit cards each with a different photograph on it, as follows:

- One of the photos was a "good, good" one. It was genuine and recent.
- The second was a "bad, good one." It was genuine but a bit old; the student now had different clothing, hairstyle, or whatever. In other words, it was typical of the photo that most people have on their photo ID.
- The third was a "good, bad one." From a pile of a hundred or so random photographs of different people, investigators chose the one that most looked like the subject. In other words, it was typical of the match that criminals could get if they had a stack of stolen cards.
- The fourth was a "bad, bad" one. It was chosen at random except that it had the same sex and race as the subject. In other words, it was typical of the match that really lazy, careless criminals would get.

The experiment was conducted in a supermarket after normal business hours, but with experienced cashiers on duty who were aware of the purpose of the experiment. Each student made several trips past the

checkout using different cards. It transpired that none of the checkout staff could tell the difference between “good, bad” photos and “bad, good” photos. In fact, some of them could not even tell the difference between “good, good” and “bad, bad.” As this experiment was done under optimum conditions—with experienced staff, plenty of time, and no threat of embarrassment or violence if a card was rejected—real-life performance can be expected to be worse. (In fact, many stores do not pass on to their checkout staff the reward offered by credit card companies for capturing stolen cards, so even the basic motivation may be absent.)

The response of the banking industry to this experiment was ambivalent. At least two banks that had experimented with photos on credit cards had experienced a substantial drop in fraud—to less than one percent of the expected amount in the case of one Scottish bank. The overall conclusion was that the benefit to be had from photo ID is essentially its deterrent effect.

In short, the technology still does not work very well, when viewed solely in terms of error rates. However, from the system viewpoint, it can work very well indeed. In 1998, the London borough of Newham placed video cameras prominently in the high street and ran a PR campaign about how their new computer system constantly scanned the faces in the crowd for several hundred known local criminals. They managed to get a significant reduction in burglary, shoplifting, and street crime. The system even worries civil libertarians—despite the fact that it appears to work primarily by deterrence. Of course, as time passes and technology improves, both the potential and the worries may increase.

### 3.4.3 Fingerprints

Fingerprints are important. By 1998, fingerprint recognition products accounted for 78% of the total sales of biometric technology. These products look at the friction ridges that cover the fingertips and classify patterns of *minutiae*, such as branches and end points of the ridges. Some also look at the pores in the skin of the ridges.

The use of fingerprints to identify people was discovered independently a number of times. Mark Twain mentioned thumbprints in 1883, in *Life on the Mississippi*, where he claims to have learned about them from an old Frenchman who had been a prison-keeper. Long before that, they were accepted in a seventh-century Chinese legal code as an alternative to a seal or a signature; and they were required by an eighth-century Japanese code when an illiterate man wished to divorce his wife. They were mentioned in work by Malpighi in Italy in the seventeenth century; and used in 1691 by 225 citizens of Londonderry in Ireland to sign a

petition asking for reparations following the siege of the city by King William.

The first modern systematic use appears to have been in India during the mid nineteenth century, when William Herschel (grandson of the astronomer) was a colonial official in Hooghly. He used fingerprints to stop impersonation of pensioners who had died, and to prevent rich criminals paying poor people to serve their jail sentences for them. Henry Faulds, a medical missionary in Japan, discovered them independently in the 1870s and brought them to the attention of Darwin, who in turn motivated Galton to work out a scheme for classifying their patterns. His classification, of *loops*, *whorls*, *arches*, and *tents*, is still in use today.

According to the English-language version of history, fingerprints passed into mainstream police use in 1900, when a former police chief from Bengal, Edward Henry, became Commissioner of the Metropolitan Police in London.

#### 3.4.4 Voice Recognition

**Voice Recognition**—also known as *speaker recognition*—is the problem of identifying a speaker from a short utterance. While *speech recognition* systems are concerned with transcribing speech and need to ignore speech idiosyncrasies, voice recognition systems need to amplify and classify them. There are many sub-problems, such as whether the recognition is text-dependent or not, whether the environment is noisy, whether operation must be real time, and whether one needs only to verify speakers or to recognise them from a large set.

In forensic phonology, a more straightforward biometric authentication objective is to verify a claim to identity in some telephone systems. These range from telephone banking to the identification of military personnel, with over a dozen systems on the market. Campbell describes a system that can be used with the U.S. government STU-III encrypting telephone, and that achieves an equal error rate of about 1%; and the NSA maintains a standard corpus of test data for evaluating speaker recognition systems.

There are some interesting attacks on these systems, quite apart from the possibility that a villain might somehow manage to train himself to imitate your voice in a manner that the equipment finds acceptable.

#### 3.4.5 Other Systems

A number of other biometric technologies have been proposed. Some, such as those based on *facial thermograms* (maps of the surface temperature of the face, derived from infrared images), the shape of the ear, gait, lip prints, and the patterns of veins in the hand, don't seem to have been marketed as products. Other technologies may provide interesting electronic in the future. For example, the huge investment in developing digital noses for quality control in the food and drink industries may lead to a "digital doggie," which recognises its master by scent.

One other biometric deserves passing mention—the use of DNA typing. This has become a valuable tool for crime-scene forensics and for determining parenthood in child support cases, but is too slow for applications such as building entry control. Being genotypic rather than phenotypic, its accuracy is also limited by the incidence of monozygotic twins—about one white person in 120 has an identical twin. There's also a privacy problem, in that it should soon be possible to reconstruct a large amount of information about an individual from their DNA sample. For a survey of forensic DNA analysis techniques, and suggestions of how to make national DNA databases consistent with European data protection law.

### 3.5 Performance Measurement

- **False Accept Rate (FAR) or False Match Rate (FMR):** This is the probability that the system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by non-allowed people.
- **False Reject Rate (FRR) or False Non-Match Rate (FNMR):** This is the probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percent of valid users who are rejected as impostors.
- **Receiver (or Relative) Operating Characteristic (ROC):** In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In real-world biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. We obtain the ROC plot by graphing the values of FAR and FRR, changing the variables implicitly. A common variation is the *Detection error trade-off (DET)*, which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

- **Equal Error Rate (EER):** It is the rate at which both accept and reject errors are equal. The best way to show the performance of a biometric system is by using a ROC or DET plot because they show clearly how FAR and FRR can be changed. However, if we want to quickly compare two systems, the EER is commonly used. It can be obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.
- **Failure to Enroll Rate (FTE or FER):** This is the percentage of people who fail to enroll in the system. Failure to enroll happens when the data obtained by the sensor are considered invalid.
- **Failure to Capture Rate (FTC):** Within automatic systems, the probability that the system fails to detect a biometric characteristic if it is presented to it correctly.
- **Template Capacity:** This is the maximum number of people it is possible to discriminate. If we use a template of  $n$  bits and if we choose the features so that each individual generates a different template, then we could ideally discriminate  $2^n$  individuals. Unfortunately, we can't find such ideal features and we have to consider noise and a certain range of uncertainty, so the actual template capacity will be much smaller than  $2^n$ .

One simple but artificial way to judge a system is by EER, but not all the authors provided it. Moreover, there are two particular values of FAR and FRR to show how one parameter can change depending on the other. For fingerprint there are two different results, the one from 2003 is older but it was performed on a huge set of people, while in 2004 much less people were involved but stricter conditions have been applied. For iris, both references belong to the same year, but one was performed on more people, the other one is the result of a competition between several universities so, even if the sample is much smaller, it could reflect better the state of art of the field.

### 3.6 Issues and Concerns

As with many interesting and powerful developments of technology, there are concerns about biometrics. The biggest concern is the fact that once a fingerprint or other biometric source has been compromised it is compromised for life, because users can never change their fingerprints. A theoretical example is a debit card with a personal Identification Number (PIN) or a biometric.

The following table shows the state of art of some biometric systems

**Table 2: State of art of biometric recognition systems**

Biometrics	EER	FAR	FRR	Subjects	Comment	Reference
<a href="#">Face</a>	n.a.	1 %	10 %	37437	Varied lighting, indoor/outdoor	FRVT (2002) <sup>[4]</sup>
<a href="#">Fingerprint</a>	n.a.	1 %	0.1 %	25000	US Government operational data	FpVTE (2003) <sup>[5]</sup>
<a href="#">Fingerprint</a>	2 %	2 %	2 %	100	Rotation and exaggerated skin distortion	FVC (2004) <sup>[6]</sup>
<a href="#">Hand geometry</a>	1 %	2 %	0.1 %	129	With rings and improper placement	(2005) <sup>[7]</sup>
<a href="#">Iris</a>	< 1 %	0.94 %	0.99 %	1224	Indoor environment	ITIRT (2005) <sup>[8]</sup>
<a href="#">Iris</a>	0.01 %	0.0001 %	0.2 %	132	Best conditions	NIST (2005) <sup>[9]</sup>
<a href="#">Keystrokes</a>	1.8 %	7 %	0.1 %	15	During 6 months period	(2005) <sup>[10]</sup>
<a href="#">Voice</a>	6 %	2 %	10 %	310	Text independent, multilingual	NIST (2004) <sup>[11]</sup>

If stolen it might allow someone else to access personal information or financial accounts, in which case the damage could be irreversible. However, this argument ignores a key operational factor intrinsic to all biometrics-based security solutions: biometric solutions are based on matching, at the point of transaction, the information obtained by the scan of a “live” biometric sample to a pre-stored, static “match template” created when the user originally enrolled in the security system. Most of the commercially available biometric systems address the issues of ensuring that the static enrollment sample has not been tampered with (for example, by using hash codes and encryption), so the problem is effectively limited to cases where the scanned “live” biometric data is hacked. Even then, most competently designed solutions contain anti-hacking routines. For example, the scanned “live” image is virtually never the same from scan to scan owing to the inherent plasticity of biometrics; so, ironically, a “replay” attack using the stored biometric is easily detected because it is too perfect a match.

The television program *Mythbusters* attempted to break into a commercial security door equipped with biometric authentication as

well as a personal laptop so equipped [\[12\]](#). While the laptop's system proved more difficult to bypass, the advanced commercial security door with “live” sensing was fooled with a printed scan of a fingerprint after it had been licked. Assuming the tested security door is representative of the current typical state of biometric authentication, that it was so easily bypassed suggests biometrics may not yet be reliable as a strong form of authentication.

### 3.7 Sociological Concerns

As technology advances, and time goes on, more and more private companies and public utilities will use biometrics for safe, accurate identification like in electronic banking transactions. However, these advances will raise many concerns throughout society, where many may not be educated on the methods. Here are some examples of concerns society has with biometrics:

- **Physical** - Some believe this technology can cause physical harm to an individual using the methods, or that instruments used are unsanitary. For example, there are concerns that retina scanners might not always be clean.
- **Personal Information** - There are concerns whether our personal information taken through biometric methods can be misused, tampered with, or sold, e.g. by criminals stealing, rearranging or copying the biometric data. Also, the data obtained using biometrics can be used in unauthorised ways without the individual's consent.

### 3.8 Danger to Owners of Secured Items

When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. In 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car.

## 4.0 CONCLUSION

The use of inanimate-centred objects in creating security measures and techniques are flawed in several ways. Therefore biometrics, which is inanimate in nature, is being deployed, more recently, in designing security and fraud detection and prevention schemes. Biometrics has proved to be efficient, but has its flaws as well. Several challenges are facing biometric applications, but these challenges are surmountable. A



synergy of biometric technologies and other forms of technology is ideal in dealing with fraudulent schemes.

## 5.0 SUMMARY

- Biometrics identifies people by measuring some aspects of individual anatomy or
- physiology (such as your hand geometry or fingerprint), some deeply ingrained skill, or other behavioral characteristic (such as your handwritten signature), or something that is a combination of the two (such as your voice).
- The modern rapid advancements in networking, communication and mobility increased the need of reliable ways to verify the identity of any person using a password. Even if we use the best encrypting algorithm, the whole security is based on the key. If it is too short, it is simple to guess it or crack it making several attempts, but if it is too complicated it can't be remembered and the common user will keep it written somewhere, so it can be lost or stolen
- Strictly speaking, *voice* is also a physiological trait because every person has a different pitch, but voice recognition is mainly based on the study of the way a person speaks, which is why it is commonly classified as behavioral.
- Handwritten signatures had been used in classical China, but carved personal seals were considered to be higher status, and are still used for serious transactions in China, Japan, and Korea to this day.
- The probability that a forged signature will be accepted as genuine mainly depends on the amount of care taken when examining it. Many bank card transactions in stores are accepted without even a glance at the specimen signature on the card—so much so that many Americans do not even bother to sign their credit cards.
- Recognising people by their facial features is the oldest identification mechanism of all, going back at least to our early primate ancestors. Biologists believe that a significant part of our cognitive function evolved to provide efficient ways of recognising other people's facial features and expressions.
- Fingerprints are important. By 1998, fingerprint recognition products accounted for 8% of the total sales of biometric technology.
- *Voice recognition*—also known as *speaker recognition*—is the problem of identifying a speaker from a short utterance.
- A number of other biometric technologies have been proposed. Some, such as those based on *facial thermograms* (maps of the surface temperature of the face, derived from infrared images), the shape of the ear, gait, lip prints, and the patterns of veins in the hand, don't seem to have been marketed as products.
- One simple but artificial way to judge a system is by EER, but not all the authors provided it.

- As with many interesting and powerful developments of technology, there are concerns about biometrics. The biggest concern is the fact that once a fingerprint or other biometric source has been compromised it is compromised for life, because users can never change their fingerprints.
- As technology advances, and time goes on, more and more private companies and public utilities will use biometrics for safe, accurate identification like in electronic banking transactions
- When thieves cannot get access to secure properties, there is a chance that they will stalk and assault the property owner to gain access.

## **6.0 TUTOR-MARKED ASSIGNMENT**

1. Identify and define human characteristics that can be used for biometrics.
2. Briefly discuss the performance measurement of biometrics.
3. Identify and define human characteristics that can be used for biometrics.
4. Briefly discuss the performance measurement of biometrics.

## **7.0 REFERENCES/FURTHER READINGS**

- Jain, A. K. (28-30 April 2004). "Biometric Recognition: How do I know Who You Are?" Signal Processing and Communications Applications Conference, 2004. Proceedings of the IEEE 12th: 3 – 5.
- Jain, A. K.; Ross, A. & Pankanti, S. (June 2006). "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security 1st (2)
- Philips, P. J. Grother, P. & Micheals, *et al.* Face Recognition Vendor Test 2002. Overview and Summary (Online).
- Wilson, C. Hicklin, A. R. & Korves, H. *et al.* Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report, NIST Internal Rep. 7123, Jun. 2004. [Online].

- Cappelli, D. Maio, D. & Maltoni, J. *et al.* (2006). "Performance Evaluation of Fingerprint Verification Systems", *IEEE Trans. Pattern Anal. Mach. Intell.*, Vol. 28, No. 1, pp. 3–18, Jan. 2006.
- E. Kukula, Elliott, S. (2005). "Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance", *IEEE* 2005.
- International Biometric Group, Independent Testing of Iris Recognition Technology, May 2005 (Online).
- NIST Iris Challenge Evaluation, (Online).
- Hocquet, S. Ramel, J. & Cardot, H. (2005). "Fusion of Methods for Keystroke Dynamic Authentication, Automatic Identification Advanced Technologies". Fourth IEEE Workshop on 17-18 Oct. 2005 Page(s):224 – 229.
- Reynolds, D. A.; Campbell, W. & Gleason, T. *et al* (2005). "The 2004 MIT Lincoln Laboratory Speaker Recognition System, in Proc.". IEEE Int. Conf. Acoustics, Speech, Signal Processing, Philadelphia, PA, Mar. 2005.
- Video of the Mythbusters Episode on how to Hack Fingerprint Scanners Vittal, N. Security, Controls And Audit in Computerized Banking Environment, NIBSCOM Seminar on 09.03.2000, New Delhi.
- BBC News: Malaysia Car Thieves Steal Finger.
- DoD Readies Biometric ID System for U.S. Bases in Iraq.

## **UNIT 3      APPLICATION OF BIOMETRICS AND ARTIFICIAL INTELLIGENCE (AI) IN ELECTRONIC FRAUD DETECTION**

### **CONTENTS**

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
  - 3.1 Voice Biometrics
    - 3.1.1 Use of Voice Biometrics in Electronic Banking: The Case of ABN AMRO
    - 3.1.2 Compliance Concerns
    - 3.1.3 Use in Fraud Busters
    - 3.1.4 Use by Government
    - 3.1.5 Potentials
  - 3.2 Hand-Written Signatures
  - 3.3 Artificial Intelligence in Fraud Detection and Prevention
  - 3.4 Challenges
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

### **1.0      INTRODUCTION**

These days, artificial intelligence and biometrics are applied in the detection and prevention of fraud in electronic banking and commerce. Several cases abound of how banks have successfully deployed biometrics and artificial intelligence to counter and checkmate fraudulent schemes. The study case of Netherlands's giant in banking ABN AMRO readily comes to mind, among other listed cases in this unit.

### **2.0      OBJECTIVES**

At the end of this unit, you should be able to:

- explain how ABN AMRO successfully deployed voice biometrics in its banking operations
- explain how some governments and organisations have also used artificial intelligence and biometrics in checking fraud
- explain challenges facing the use of biometrics and artificial intelligence.

### **3.0      MAIN CONTENT**

### **3.1 Voice Biometrics**

#### **3.1.1 Use of Voice Biometrics in Electronic Banking: The Case of ABN AMRO**

Trial deployments are still the norm, but banks like ABN AMRO have already moved beyond the trial stage and are rolling out voice biometrics in an effort to reduce fraud, boost security and lower costs. Zsolt Kadar, an IT project manager for the bank, said that the main customer call center in the Netherlands serves 4 million Dutch customers, and those 4 million customers make 35 million calls a year to the bank. When customers call, they are required to enter a five-digit code to verify their identities—essentially, it's a PIN number, but it's a different PIN number from the one used for ATM transactions. This makes the system more secure, but customers keep forgetting or losing the code since they use it so infrequently. This has happened even to Kadar. And when it happens, the bank has to issue a new telephone code—an expensive proposition.

Once a person's voice is enrolled in a voice biometrics security system, the need for this extra number goes away. The bank saves money, and customers are less frustrated—especially important for a country like the Netherlands, where the average customer now goes to the local branch on average only once a year.

Most banking is now done by phone, Internet, and ATM, and criminals—like electrical current—will always choose the path of least resistance. It doesn't matter how hardened a bank's ATM security measures are or how robust the SSL system it uses on the Internet is if phone banking remains less secure. So ABN AMRO went shopping for a voice biometric system that would help them boost security and eliminate the telephone code. They settled on a system from Voice Vault that showed good results at handling many types of phones. The system measures 117 characteristics of the human voice which can detect recordings using a dynamic voice model that updates the stored voiceprint after every successful verification because voices can change over time.

The bank then embarked on the largest worldwide experiment with voice biometrics, using 1,450 people to make more than 30,000 calls to the test system. The testers called from every sort of phone imaginable, in every setting. They called when they had colds; they had family members call and attempt to impersonate them; they used recordings of their own voice to try and fool the system. After tuning the software for ABN AMRO's particular needs, Voice Vault achieved an EER of below one percent—and that's without factoring in the secret question.

When testers first called into the system, they were "enrolled": that is, several voice samples were taken, and a voiceprint was generated. The testers also created their own secret questions, recording both a question and an answer. When they called back, the system prompted them to say their account number and to answer the secret question. The new voice sample was checked against the stored voiceprint information in real time and the answer to the secret question was checked against the stored sample. Imposters who knew the account number, and the answer to the question still failed the voice check. Only if the account number and secret question were correct and the voice matched was the caller allowed to proceed.

Are customers ready for this technology? Kadar believes that they are. ABN AMRO did a survey of those who tested the system and found that 83 percent of them preferred voice verification to the older five digit code. 99 percent said they would feel comfortable using the system to access account information and 73 percent had no problem using it for money transfers. Based on its results, the bank is deploying the system in the Netherlands on a voluntary basis this year and next; customers who don't feel comfortable using it can continue to use the five-digit code for now.

### **3.1.2 Compliance concerns**

Voice systems aren't just getting a boost from their cost and security; they're also getting a boost due to regulatory pressure. In the US, the Federal Financial Institutions Examination Council (FFIEC) issued guidance to banks in late 2005 (PDF) on the use of security in Internet environments. The group later clarified that this guidance extended to telephone banking systems. Jeffrey Kopchik, a senior policy analyst at the FDIC, was on hand at the conference to explain the guidance in a bit more detail.

While the FFIEC did not mandate multifactor authentication, the guidance does require that financial institutions use more security than a user ID and password combination. Voice verification is an excellent way to comply with the guidance, but Kopchik pointed out that such systems cannot remain optional or they would defeat the whole point of the new rules; banks must require users to shift to sign-in methods that meet the more stringent authentication requirements.

But voice verification systems are only as good as their enrollment procedures. It does no good for a system to be hyper-accurate in matching callers to stored voiceprints if the original voiceprint was not made from the right person. This poses a challenge that different

institutions meet in different ways; ABN AMRO relies on a small electronic gadget that customers receive in the mail or at a local branch. When they insert their bank card into the top of the device, a string of numbers appear on the small screen. They then use these numbers to verify themselves to the bank.

Once enrollment in the system is completed, this step does not have to be done again, but what happens to those people who can't enroll? Every voice verification system comes across certain users (called "goats" at some firms) whose voices simply cannot be turned into voiceprints by the algorithms. And then there are those who can't hear or can't speak; all telephone-based systems need to have some alternate means of communicating with these customers.

### **3.1.3 Use in Fraud Busters**

Governments not only issue guidance on security protocols, but they use them, too. In Australia, the national government has already implemented voice verification systems in multiple agencies. Politicians who needed to access sensitive documents from secure servers in a regular basis have problems remembering their passwords, so a voice verification system was ruled out in the Parliament House that allows the prime minister and cabinet members to access documents with their voices.

Dr. Summerfield, the University of Canberra researcher, also pointed out that voice verification can be used for a different kind of fraud detection. A voice biometric system was installed for Australian social security agency Centrelink a few years back, as the agency handles over 100,000 phone calls per day at the largest call center in the southern hemisphere. 85 percent of those calls need to be authenticated, and under the old system, this was taking too much time.

Centrelink installed a voice verification system simply to authenticate users, but once it was in place, realised that it could also be used to look for particular kinds of fraud: speakers who change from one reporting period to the next, or a single speaker accessing multiple accounts (in order to gain multiple benefits). An initial sweep of the data that was already being gathered for authentication purposes, found 20 pairs of "non-compliant speakers"—two or more people quoting the same ID number. More serious were the 200 cases of suspected ID fraud, where one person knew multiple ID numbers and was attempting to access benefits for each of them.

Older systems that rely than punching numbers into a telephone keypad or that forced people to speak with a live operator could not tell if

different people were calling up on the same account each month, or if the same person was accessing multiple accounts. The new biometric system records the necessary information as part of its regular duties, and all that's left is to run searches against the database. Centrelink's conclusion was that the system was very useful for fraud detection, and it may continue to use it for this purpose.

### **3.1.4 Use by Government**

With governments and major private institutions beginning to collect databases of voiceprints, certain privacy concerns are inevitably raised. Michael Kramer, the CEO of Voice -Trust, described his own attempt to sell his company's voice biometrics software in France. It took 18 months of negotiations with French regulators, and it culminated in a meeting in Paris where Kramer was grilled by government officials about whether his company might ever provide voiceprints to the CIA or related entities.

In the US, similar questions might be asked of corporations, even those with strict privacy policies, in the wake of the phone companies' capitulation to the US government regarding phone records. Should an intelligence agency or even a police department find themselves with a juicy piece of audio evidence that they can't match up to a name, it doesn't require a huge imaginative leap to see that they might be tempted to secure private databases from banks and other institutions in order to find a match. While that doesn't sound too bad, it could eventually lead to government in possession of massive voiceprint databases that could identify a large percentage of US speakers.

Is that a bad thing? The answer to that depends on your politics. It would also be a ton of work for the government to do such a thing, since the various voiceprints would all be generated in different ways and stored in different formats. Consolidating them into some national database of speakers would require substantial time and energy and, quite possibly, cooperation from the five or six companies that design the core verification engines.

### **3.1.5 Potentials**

Voice verification is here at last and poised to grow rapidly, but it's still a small market. All forms of biometric identification generated \$2 billion of revenue in 2006, according to Dan Miller, a senior analyst at Opus Research—and half of that money went to fingerprint scanning. But voice, due to particular passages we've been discussing, has already won over ABN AMRO, Bell Canada, Ameritrade, the Australian



government, Volkswagen Financial Services, and (of all things) the US Department of Agriculture.

Dan Faulkner, the director of product management and solution marketing at Nuance, tells Ars that his company's systems have achieved tuned errors of below one percent in real-world deployments with companies like [Aeroplan](#), and other vendors reported similar results in their own deployments. When voice verification is text-dependent, this error rate is further reduced by orders of magnitude. The systems can be quite secure, but they do have their limits.

One of those limits is twins and even immediate family members, whose physiology may be similar enough to confuse the computer. Oliver Geiseler of Volkswagen Financial Services described his own company's use of voice verification for an internal help desk password reset application. Twins, it turns out, were able to defeat the system.

This isn't the sort of thing that keeps security researchers up at night, but it's a reminder that the systems aren't perfect and probably never will be. The hardest choice for companies that roll out the technology isn't finding a decent vendor or a robust implementation, but deciding how much risk they can tolerate, and how much frustration their customers will accept in the name of tighter security.

### **3.2 Handwritten Signatures**

The probability that a forged signature will be accepted as genuine mainly depends on the amount of care taken when examining it. Many bank card transactions in stores are accepted without even a glance at the specimen signature on the card—so much so that many Americans do not even bother to sign their credit cards. (This can cause problems when traveling in more punctilious countries such as Germany or Switzerland.) But even diligent signature checking doesn't reduce the risk of fraud to zero. An experiment showed that 105 professional document examiners, who each did 144 pair-wise comparisons, misattributed 6.5% of documents. Meanwhile, a control group of 34 untrained people of the same educational level got it wrong 38.3% of the time, and the nonprofessionals' performance couldn't be improved by giving them monetary incentive. Errors made by professionals are a subject of continuing discussion in the industry, but are thought to reflect the examiner's assumptions and preconceptions. As the participants in these tests were given reasonable handwriting samples rather than just a signature, it seems fair to assume that the results for verifying signatures on checks or credit card vouchers would be significantly worse.

There is one application where effective automatic recognition of handwritten signatures could be very valuable. This is check clearing. In a bank's check processing center, it is typical practice that you only verify signatures on checks over a certain amount—perhaps \$1,000, perhaps \$10,000, perhaps a percentage of the last three months' movement on the account. The signature verification is done by an operator who sees, simultaneously presented on-screen, the check image and the customer's reference signature.

Verifying checks for small amounts is not economic unless it can be automated, so a number of researchers have worked on systems to compare handwritten signatures automatically. This turns out to be a very difficult image-processing task because of the variability between one genuine signature and another. A much easier option is to use a *signature tablet*. This is a sensor surface on which the user does a signature; it records not just the shape of the curve but also its dynamics (the velocity of the hand, where the pen was lifted off the paper, and so on). Tablets are used to identify users in some high-value applications, including securities dealing.

Like alarm systems, most biometric systems have a trade-off between false accept and false reject rates, often referred to in the banking industry as the *fraud* and *insult* rates, and in the biometric literature as *type 1* and *type 2* errors. Many systems can be tuned to favor one over the other. The *equal error rate* is when the system is tuned so that the probabilities of false accept and false reject are equal. For common signature recognition systems, the equal error rate is about 1%. This is not fatal in an operation such as a bank dealing room. If one of the dealers tries to log on one morning and his PC rejects his signature, he can just try again. If there is a persistent failure, he can call the system administrator and have the machine reset. However, it is a show-stopper in a retail store. If one transaction in a hundred fails, the aggravation to customers would be unacceptable. So U.K. banks set a target for biometrics of a fraud rate of 1% and an insult rate of 0.01%, which is beyond the current state of the art in signature verification.

In general, biometric mechanisms tend to be much more robust in attended operations, where they assist a guard rather than replacing him. The false alarm rate may then actually help by keeping the guard alert.

### 3.3 Artificial Intelligence in Fraud Detection and Prevention

**Case 1:** When a credit card use has been queried, it's probably because more banks are now using artificial intelligence software to try to detect fraud. Credit card fraud losses in the UK fell for the first time in nearly a decade last year, by more than 5% to 402.4m [British pounds],

according to research by the Association of Payment Clearing Services (Apacs). The fall has put a spotlight on the increasing use of neural networks that have the ability to detect fraudulent behaviour by analysing transactions and alerting staff to suspicious activity. As commercial applications of research into artificial intelligence, these systems give the impression of mimicking human abilities for recognising unusual activity. Karina Purang, a financial analyst at Data monitor in London, says the use of neural networks is growing: "These systems are very important to banks trying to reduce fraud, and are becoming standard across the card industry to detect unusual spending patterns." She says Barclays reported that after installing Fair Isaac's Falcon Fraud Manager system in 1997, fraud was reduced by 30% by 2003. The bank attributed this mainly to the new system. Nick Sandall, head of retail banking at Deloitte, says that banks also use other technologies. "The artificial intelligence community is constantly bringing us new solutions. ..."

**Case 2:** Computer sleuths trying to stop health care fraud say they have a new weapon: computer programs that can flag potential fraud even before medical claims are paid. Insurer Aetna says its new computer software helped it stop \$89 million in payments before they reached medical providers last year. That compares with the \$15 million in fraud repayments it was able to collect after the fact. While the software systems may differ, their main effort is to spot medical providers who vary from the norm. "Pattern recognition is a growing field in health fraud detection," says Malcolm Sparrow, a professor at Harvard's John F. Kennedy School of Government and author of *License to Steal: How Fraud Bleeds America's Health Care System*.

**Case 3:** Today, an electronic brain is helping to cut credit card fraud. There is a lot of identity theft lately, but it is surprising to learn that credit card fraud is actually declining. Nearly all transactions for Visa, MasterCard, American Express and others are scrutinised electronically before they're approved. David Robertson, publisher of the credit industry's Nilson Report, explains. While it's going through their system for authorisation, it's also being checked against information about previous spending. So if you use your card in a location say, Seattle in the morning and someone tries to use the same account an hour later in another location like, New York, the security system will send up a big red flag. Credit card companies use what is essentially an electronic brain, aided by a form of artificial intelligence known as neural networks. The brain keeps track of every purchase you make and sorts them into patterns and categories and compares your spending habits to others and to credit card activity linked to fraudsters. Then it makes predictions about whether a transaction is legitimate or not.

**Case 4:** Companies in health care, finance, and retailing are using artificial-intelligence systems to filter huge amounts of data and identify suspicious transactions. Banks, brokerages, and insurance companies have been relying on various AI tools for two decades. One variety, called a **neural network**, has become the standard for detecting credit-card fraud. Since 1992, neural nets have slashed such incidents by 70% or more.

**Case 5:** UK-based Future Route is releasing a new card fraud detection system, IHex, based on artificial intelligence technology developed at Oxford University's computing laboratories for bio-informatics. The product has been designed for use by financial services firms, government agencies and corporations. IHex detects fraud using Inductive Logic Programming (ILP) techniques - an artificially intelligent method of identifying fraud patterns and anomalies. The vendor says unlike many other pattern detection products, the system automatically generates and continuously enhances underlying rules.

**Case 6:** With billions of dollars at stake, and more clever crooks, credit card companies have become very smart about protecting themselves with astonishingly sophisticated network computers and software programs. According to Raf Sorrentino, vice president of risk management for First Data Corporation, one of the biggest providers of credit card processing and payment services; *"We're at a level whereby we can understand with artificial intelligence ... the potentially fraudulent transactions"*. Credit card fraud costs the industry about a billion dollars a year, or 7 cents out of every \$100 spent on plastic. But that is down significantly from its peak about a decade ago, Sorrentino says, in large part because of powerful technology that can recognise unusual spending patterns.

**Case 7:** *Monitoring NASDAQ for Potential Insider Trading and Fraud.* NASD has developed an intelligent surveillance application - the Securities Observation, News Analysis and Regulation (SONAR) system - that automatically monitors the NASDAQ, OTC, and futures markets for suspicious patterns. SONAR includes several AI techniques, such as data mining, natural language processing for text mining, intelligent software agents, rule-based inference, and knowledge-based data representation.

**Case 8:** *The Financial Crimes Enforcement Network AI System (FAIS). Identifying Potential Money Laundering from Reports of Large Cash Transactions;* The Financial Crimes Enforcement Network (FIN-CEN) AI system (FAIS) links and evaluates reports of large cash transactions to identify potential money laundering. The objective of FAIS is to discover previously unknown, potentially high-value leads for possible

investigation. FAIS integrates intelligent human and software agents in a cooperative discovery task on a very large data space. It is a complex system incorporating several aspects of **AI technology**, including rule-based reasoning and a blackboard. FAIS consists of an underlying database (that functions as a black-board), a graphic user interface, and several preprocessing and analysis modules. FAIS has been in operation at FINCEN since March 1993; a dedicated group of analysts process approximately 200,000 transactions a week, during which time over 400 investigative support reports corresponding to over \$1 billion in potential laundered funds were developed.

### 3.4 Challenges

As with other aspects of security, we find the usual crop of failures in biometrics due to bugs, blunders, and complacency. The main problem faced by DNA typing, for example, was an initially high rate of false positives, due to careless laboratory procedure. This not only scared off some police forces, which had sent in samples from different volunteers and got back false matches, but also led to disputed court cases and alleged miscarriages of justice.

Biometrics is like many other protection mechanisms (alarms, seals, tamper sensing enclosures ...) in that environmental conditions can cause havoc. Noise, dirt, vibration, and unreliable lighting conditions all take their toll. Some systems, like speaker recognition, are vulnerable to alcohol intake and stress. Changes in environmental assumptions, such as from closed to open systems, from small systems to large ones, from attended to standalone, from cooperative to recalcitrant subjects, and from verification to identification—can all undermine a system's viability.

There are a number of more specific and interesting attacks on various biometric systems.

- There have been some attacks on the methods used to index biometric data.

The classic one is the helpful villain who gives an inexperienced policeman his fingerprints in the wrong order, so that instead of the hand being indexed under the Henry system as “01101” it becomes perhaps “01011”, so his record isn't found and he gets the lighter sentence due a first offender.

- Forensic biometrics often doesn't tell as much as one might assume. Apart from the possibility that a fingerprint or DNA sample might have been planted by the police, it may just be old. The age of a

fingerprint can't be determined directly, and prints on areas with public access say little. A print on a bank door says much less than a print in a robbed vault. So in premises vulnerable to robbery, cleaning procedures may be critical for evidence. If a suspect's prints are found on a bank counter, and she claims to have gone there three days previously, she may be convicted by evidence that the branch counter is polished every evening. Putting this in system terms, freshness is often a critical issue, and some quite unexpected things can find themselves inside the "trusted computing base.

- Another aspect of freshness is that most biometric systems can, at least in theory, be attacked using suitable recordings. We mentioned direct attacks on voice recognition, attacks on iris scanners by photos on a contact lens, and molds of fingerprints. Even simpler still, in countries where fingerprints are used to pay pensions, there are persistent tales of "Granny's finger in the pickle jar" being the most valuable property she bequeathed to her family. This reinforces the lesson that unattended operation of biometric authentication devices is tricky.
- Certain systems—notably handwriting systems—are vulnerable to collusion. Villains can voluntarily degrade handwriting ability. By giving several slightly different childish sample signatures, they can force the machine to accept a lower threshold than usual. The kind of attack to expect is that Alice opens a bank account and her accomplice Betty withdraws money from it; Alice then complains of theft and produces a watertight alibi. As with alarm and shared control systems, commercial users have to worry about colluding employees or customers, while the military threat model is usually just the single disloyal soldier.
- Commercial system builders must also worry about false repudiation—such as whether a user who practices enough can generate two signatures that pass for identical on the signature tablet, even if they are visually quite different.
- The statistics are often not understood by system designers, and the birthday theorem is particularly poorly appreciated. With 10,000 biometrics in a data- base, for example, there are about 50,000,000 pairs. So even with a false accept rate of only one in a million, the likelihood of there being at least one false match will rise above one-half as soon as there are somewhat over a thousand people (in fact, 1,609 people) enrolled. So identification is a tougher task than verification. The practical consequence is that a system designed for authentication may fail when you try to rely on it for evidence. A good way to explain to judges, and other non-technical people, why

the system error rate differs from the single sample error rate is that there is “one chance to get it right, but  $N$  chances to get it wrong.” For a good discussion of error rates see.

- Another aspect of statistics comes into play when designers assume that by combining biometrics they can get a lower error rate. The curious and perhaps counter-intuitive result is that a combination will typically result in improving either the false accept or the false reject rate, while making the other worse. One way to look at this is that if you install two different burglar alarm systems at your home, then the probability that they will be simultaneously defeated goes down while the number of false alarms goes up. In some cases, such as when very good biometrics is combined with a very imprecise one, the effect can be worse overall.
- Most biometrics is not as accurate for all people, and some of the population can't be identified as reliably as the rest (or even at all). The elderly, and manual workers, often have damaged or abraded fingerprints. People with dark colored eyes and large pupils give poorer iris codes. Disabled people, with no fingers or no eyes, risk exclusion if such systems become widespread. Illiterates who make an “X” are more at risk from signature forgery.
- Finally, Christian fundamentalists are uneasy about biometric technology. They find written of the Antichrist in Revelation 13:16-17: “And he causes all, both small and great, rich and poor, free and slave, to receive a mark on their right hand or on their foreheads, and that no one may buy or sell except one who has the mark or the name of the beast, or the number of his name.” So biometrics can arouse political opposition on the right as well as the left. So there are some non-trivial problems to be overcome before biometrics will be ready for mass-market use, in the way that magnetic strip cards are used at present. But despite the cost and the error rates, they have proved their worth in a number of applications, most notably where their deterrent effect is useful.

## 4.0 CONCLUSION

The application of biometrics and artificial intelligence in fraud detection in electronic banking and commerce has given some measure of confidence to electronic business operators. The combination of these new measures and the conventional methods of fraud detection and prevention will further instill confidence in investors who like to patronise electronic transaction product and services. These seemingly new wave of fraud detection measure is not without flaws, but these

flaws can be minimised to harness the full potentials of biometrics and artificial intelligence in fraud detection.

## 5.0 SUMMARY

- Over the last quarter century or so, people have developed a large number of biometric devices; this rapidly growing market is now worth about \$50 million a year.
- Once a person's voice is enrolled in a voice biometrics security system, the need for this extra number goes away. The bank saves money, and customers are less frustrated—especially important for a country like the Netherlands, where the average customer now goes to the local branch on average only once a year.
- When a credit card use has been queried, it's probably because more banks are now using artificial intelligence software to try to detect fraud. Credit card fraud losses in the UK fell for the first time in nearly a decade last year, by more than 5% to 402.4m.
- The probability that a forged signature will be accepted as genuine mainly depends on the amount of care taken when examining it. Many bank card transactions in stores are accepted without even a glance at the specimen signature on the card—so much so that many Americans do not even bother to sign their credit cards.
- Computer sleuths trying to stop health care fraud say they have a new weapon: computer programs that can flag potential fraud even before medical claims are paid.
- Today, an electronic brain is helping to cut credit card fraud. There is a lot of identity theft lately, but it is surprising to learn that credit card fraud is actually declining.
- Forensic biometrics often doesn't tell as much as one might assume. Apart from the possibility that a fingerprint or DNA sample might have been planted by the police, it may just be old.
- With billions of dollars at stake, and more clever crooks, credit card companies have become very smart about protecting themselves with astonishingly sophisticated network computers and software programs.
- As with other aspects of security, we find the usual crop of failures in biometrics due to bugs, blunders, and complacency.
- Certain systems—notably handwriting systems—are vulnerable to collusion.
- Commercial system builders must also worry about false repudiation—such as whether a user who practices enough can generate two signatures that pass for identical on the signature tablet, even if they are visually quite different.
- Christian fundamentalists are uneasy about biometric technology.



## 6.0 TUTOR-MARKED ASSIGNMENT

1. Mention and discuss 5 challenges facing the use of biometrics and artificial intelligence in fraud detection.
2. Mention and discuss 2 cases where artificial intelligence has been used to forestall fraud.

## 7.0 REFERENCES/FURTHER READINGS

Anderson, Nate (2007). *Voice Biometrics: Coming To a Security System Near You*.

Anderson, Nate (2007). *Voice Biometrics: Big Brother is Listening to You*.

Vittal, N. "Security, Controls and Audit in Computerized Banking Environment". NIBSCOM Seminar on 09.03.2000. New Delhi.

## **UNIT 4      IDENTIFYING AND RESPONDING TO ELECTRONIC FRAUD RISKS: *THE CASE OF AUSTRALIA***

### **CONTENTS**

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
  - 3.1 Circumstances and Types of Fraud
  - 3.2 Electronic Funds Transfer Crime
  - 3.3 Electronic Funds Transfer Crime
  - 3.4 Identity-Related Crime
  - 3.5 On-line Share Market Manipulation
  - 3.6 Risk Factors and Anomalies
  - 3.7 Responding to Fraud Risks
    - 3.7.1 Effective Corporate Governance
    - 3.7.2 Fraud Control Policies
    - 3.7.3 Personnel Monitoring
    - 3.7.4 Computer Usage Monitoring
  - 3.8 The Consequences of Failure to Respond to Fraud within Organisations
  - 3.9 Recommendations
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Readings

### **1.0 INTRODUCTION**

Fraud involves the use of dishonest or deceitful conduct in order to obtain some unjust advantage over someone else. Fraud costs the Commonwealth Government several million dollars yearly. It costs big business organisations huge sums of money. The Australian Institute of Criminology once said it was ready to release data from a study of crime against small business, which showed that fraud costs small business more in dollar terms than employee theft, burglary, armed robbery, unarmed robbery, and vandalism.

The prevention and control of fraud have been two great challenges for Australia now, and in years to come. It has been around for as long as people have been around - somebody trying to con somebody else, to offer them an unbelievable and unattainable deal, or to work the system unlawfully to their own advantage so that things come incredibly easily. While crimes of deception are well-established in history, technological,

social, demographic and economic developments have brought about changes in the form fraud takes and how it is perpetrated.

## **2.0 OBJECTIVES**

At the end of this unit, you should be able to:

- explain what fraud is and circumstances that bring about fraud
- identify the various types of fraud
- explain the question of risk factors associated with fraud schemes
- identify how to deal with fraud in organisations
- explain the consequences of not effectively tackling fraud in corporate organisations as well as in government.

## **3.0 MAIN CONTENT**

### **3.1 Circumstances and Types of Fraud**

The circumstances in which fraud can exist are enormously diverse. Some of the types include: commercial fraud, fraud against governments, consumer fraud, migration fraud, securities fraud, superannuation fraud, intellectual property fraud, computer and telecommunications fraud, insurance fraud, plastic card fraud, art fraud, charitable contribution fraud, identity-related fraud, advance fee fraud, health care fraud, and the list goes on and on, and new opportunities for deceptive conduct arise all the time.

The basic motivation for fraud is greed, a fairly robust and enduring human characteristic. We are unlikely to eliminate greed in my lifetime or yours, so countermeasures have to be more than psychological or feel good tactics. Crime follows opportunity, and opportunities for fraud flow from economic growth. The more commerce there is, the more opportunities there are to commit fraud. Nobody wants to pull the plug on electronic commerce, close down the stock market, or the health insurance system, just because they may be vulnerable to fraud.

The area of concern closest to your interests relates to the opportunities for fraud that arise out of electronic service delivery. In the past, sophisticated paper-based systems were present to reduce the opportunities for fraud. As we move into online registration of titles and electronic transactions, new opportunities arise for people within organisations as well as for external customers to misrepresent themselves and to manipulate electronic transactions for financial gain.

The challenge lies in designing systems, which allow commerce to flourish while blocking opportunities for fraud. This challenges us to

extend our ingenuity to counter that of villains, and to build smart systems. Like all crimes, fraud is the product of three factors:

- Motivation - somebody willing to offend
- The presence of a prospective victim or target
- The absence of a capable guardian.

This general rule applies whether we are referring to fraud against a government benefits programme, fraud against elderly people, fraud against your organisation, or misappropriation of corporate assets by a company director. Three ways to work on the limitation of fraud involve:

- Reducing the supply of motivated offenders
- Protecting and educating the suitable targets
- Limiting opportunities by making the crime more difficult to commit

We shall focus only on 3 types of examples that raise issues relevant to electronic conveyance.

### **3.2 Electronic Funds Transfer Crime; Identity-Related Crime; Online Share-Market Manipulation**

The techniques that have been used to commit fraud in these areas are exactly the same as those that could be used to attack the Offices of Titles around the country (that is Australia). While fraud has been around forever, the common thread running through most of the current wave of economic crimes is that they are greatly facilitated by recent developments in information technology.

The benefits of computing and communications technologies are clearly apparent. People are able to communicate more effectively and at lower cost than in the past. It has also meant that geographical boundaries are able to be crossed more easily which has enhanced the process of globalisation of economic and social life enormously. These same technologies that have provided so many benefits have, however, created enormous opportunities for offenders—Criminals are able:

- to communicate with each other in secret,
- to disguise their identities in order to avoid detection,
- to counterfeit and alter documents using desk-top publishing equipment; and
- to manipulate electronic payment systems to obtain funds illegally.

They are also able to perpetrate fraud on a much wider scale than in the past, duplicating countless fraudulent invoices, or establishing large

numbers of accounts that only exist in cyberspace. Their victims may also be located anywhere in the world.

### **3.3 Electronic Funds Transfer Crime**

All companies and organisations move money electronically. In the olden days, law clerks would stand in line at the Titles Office and hand a piece of paper over to an officer at the counter who probably knew the person by sight, and if there was an anomaly, it would be picked up by the official who just knew!

Crime today takes place by manipulating the security systems established to protect electronic funds transfers. These systems are designed to ensure that information cannot be manipulated as it passes over computerised networks and that only authorised users have access to computers. Law clerks of the future will spend their time in the office in front of a screen rather than physically walking to the Titles Office to lodge documents and to pay fees.

Most of the large scale electronic funds transfer frauds which have been committed in the past have involved the interception or alteration of electronic data messages transmitted from the computers of financial institutions.

In many cases offenders have worked within financial institutions or corporations themselves and been privy to the operation of the security systems in question. One example of funds transfer fraud involved a financial consultant contracted to the Department of Finance and Administration in Canberra who, on 25 September 2001 was convicted of defrauding the Commonwealth by transferring A\$8,735,692 electronically to private companies in which he held an interest. He did this by logging on to the department's computer network using another person's name and password. He also was able to obscure an audit trail by the use of other employees' logon codes and passwords. He was sentenced in the ACT Supreme Court to 7 ½ years imprisonment. Could this sort of thing happen in your organisation?

### **3.4 Identity-Related Crime**

In the old days bushrangers and outlaws used masks to cover their faces so nobody would know who they were. Today, on the Internet, nobody really knows who you are. One of the most frequently used strategies to perpetrate crime is the creation of false documents used to misrepresent one's identity. Once a convincing identity has been fraudulently established, it is then possible to defraud organisations, steal funds and then to evade detection, investigation, and arrest.

Stealing identities, or creating false identities, pervades every aspect of our life. At the benefit concert in New York to raise money for families of the emergency services victims killed in the World Trade Centre attacks, the legendary British rock group, The Who brought the audience to their feet with a rousing rendition of their classic song “Who are you”. At the time however, neither the band nor the audience, were aware of just how significant the timing of this song was. Even as it was played, the FBI was busy with the added burden of a new and rapidly escalating economic crime directly related to the New York tragedy.

Within days of the appearance of lists of those missing – or presumed missing – in the rubble of Manhattan, hundreds of millions of dollars of goods and services were being illegally obtained by people who had adopted the identities of the victims. Such was the out pouring of public sympathy that people were literally able to walk in off the street into government offices, shops and banks, report that their usual documentation was lost in the rubble, and on the production of the flimsiest of identification, obtain documentation like real driver’s license, which in turn were then used to obtain other genuine documents.

From here, it was only a short step to illegally obtaining goods and services, such as opening up lines of credit large enough to drive away in brand new and expensive cars. False identity was also an issue on September 11 in that nobody knew for a long time who it was who was flying those planes, how they got into the country etc. This example is grotesque under the circumstances but it highlights in graphic detail a problem of identity theft - a crime which is the boom crime of our times. The risks of identity-related fraud associated with electronic conveyance are great as the most sophisticated security systems that protect data as they are transmitted electronically across telephone lines or via satellites are of little protection, if someone simply adopts a false identity, perpetrates a fraud and then is unable to be located by the police obtaining cryptographic key pairs for use in a Public Key system. Title Offices of the future will use, by presenting false proof of identity documents and would be the easiest way in which to perpetrate conveyance fraud in the future.

Similarly, if internal staff uses other people’s passwords to enter networks to which they do not have authorisation, this may create enormous opportunities for fraud to occur. Finally, there is the possibility that staff within Registries may be subject to bribery or duress by individuals seeking to gain access to secure systems. In this way, security systems can be overcome by resorting to the potential for corruption from within agencies.

### **3.5 Online Share-Market Manipulation**

An illustration of the risks that online service delivery can entail is electronic share trading. The use of computers and e-mail has greatly facilitated the manipulation of share markets during secondary trading of securities. This can occur through the use of rumour, hyperbole, or other forms of misinformation to boost the price of a stock prior to the manipulator's quick and profitable exit ("pump and dump"), or by talks down a stock so that he or she may buy in at a bargain price ("slur and slurp").

In an Australian prosecution, a 24 year-old man who lived in a Melbourne suburb, manipulated the share price of an American company by posting information on the Internet and sending e-mail messages around the globe that contained false and misleading information about the company. On 8 and 9 May 1999, he posted messages on Internet Bulletin Boards in the United States and sent more than four million unsolicited e-mail messages to recipients in the United States, Australia and in other parts of the world. The messages contained a statement that share value of the company would increase from the then current price of US\$0.33 to US\$3.00 once pending patents were released by the company, and that the price would increase up to 900 per cent within the next few months.

The effect of the information was that the company's share price on the NASDAQ doubled, with trading volume increasing by more than ten times the previous month's average trading volume. The offender had purchased 65,500 shares in the company through a stock broking firm in Canada several days before he transmitted the information. He sold the shares on the first trading day after the transmission of the information and realised a profit of approximately A\$17,000. The offender was prosecuted by the Australian Securities and Investments Commission for distributing false and misleading information with the intention of inducing investors to purchase the company's stock. He pleaded guilty and was sentenced to two years' imprisonment on each of three counts, to be served concurrently. The Court ordered that twenty-one months of the sentence be suspended upon his entering into a two-year-good-behaviour bond with a surety of \$500.

### **3.6 Risk Factors and Anomalies**

These are only some of the types of fraud facing Australian organisation today. Before discussing what to do about it, you have to know that you're being scammed. This is not nearly as obvious as it sounds, and often does not come to light until late in the piece -often too late! There

are certainly some risk factors, and some red flags. Always look for anomalies - in essence, there are three types of anomalies to look out for, behavioural anomalies, statistical anomalies and organisational anomalies.

- **Behavioural** anomalies can be found in people suddenly changing their lifestyles, living beyond their means - they might have come into a lot of money legitimately, but keep an eye out for behavioural anomalies.
- **Statistical** anomalies are when the numbers don't look right, expenses claims out of whack with past patterns, sudden changes in credit card bills, tax deductions out of proportion to income, insurance claims that bear no resemblance to a person's lifestyles etc.
- **Organisational** anomalies are activities which diverge notably from best practice -inadequate systems of communication within the organisation, lack of transparency to outside observers, the absence of financial control systems, the Board of Directors handpicked by the CEO, poor leadership, inflated financial targets, unrealistic incentive structures based on commissions are all risk signals.

### 3.7 Responding to Fraud Risks

The absence of anomalies, however, does not mean the absence of fraud. How, then should corporations respond to these risks? Let me outline four general preventive strategies:

- Effective corporate governance
- Fraud control policies
- Personnel monitoring
- Computer usage monitoring

These however are a backdrop to the hard approach - using a range of technologies to prevent corporate fraud, or using the criminal justice system to prosecute and punish offenders.

#### 3.7.1 Effective Corporate Governance

In the first place it is important for those who manage organisations to have a proper understanding of the risks that are present within their organisations. This requires managers to know precisely how their business operates. Often those in charge of companies may not understand how their organisations function in sufficient detail to be fully aware of the risks of fraud that exist. This is particularly the case with respect to information technologies. In Ernst and Young's survey



of large organisations for example, less than one third of the Australian respondents considered that their directors had a good overall understanding of their business for fraud prevention purposes. Although managers may not be able to understand the technicalities of all the computer software and hardware that their organisations make use of, they should be in a position to understand the areas where fraud risks arise and instruct appropriately trained personnel to monitor these areas regularly.

### **3.7.2 Fraud Control Policies**

It is also important for organisations to have clear and transparent fraud control policies in place. These are necessary in the digital environment no less so than in the terrestrial world. Australian Standard No. AS 3806-98 *Compliance Programs* provides guidelines for both private and public sector organisation on the establishment, implementation and management of effective compliance programs. The Standard also provides principles which organisations are able to use to identify and to remedy any deficiencies in their compliance with laws, industry codes and in-house company standards, and to develop processes for continuous improvement in risk management.

Establishing principles on, for example, the ethical use of information technologies and how to respond to instances of fraud are essential in conducting a business of any kind, whether or not it makes use of electronic commerce. Of particular importance is the need to develop specific policies on computer security along with appropriate guidelines on reporting computer misuse and abuse. Policies need to deal with specific on-line behaviour of employees such as security of user authentication systems (e.g. passwords), access to and use of the computers for private purposes, personal use of electronic mail, downloading software, and the use of copyright material. Principles also need to be established to ensure that those who report illegal conduct are not disadvantaged by their conduct.

### **3.7.3 Personnel Monitoring**

There is also a need for organisations to be confident that the staff they are employing are reliable and trustworthy, as electronic fraud often involves confederates with inside knowledge of a company's security and computer procedures. The administration of modern technologically-based security systems involves a wide range of personnel from those engaged in the manufacture of security devices to those who maintain sensitive information concerning passwords and account records. Each has the ability to make use of confidential information or facilities to commit fraud or, what is more likely to

occur, to collude with people outside the organisation to perpetrate an offence.

Preventing such activities requires an application of effective risk management procedures which extend from pre-employment screening of staff to regular monitoring of the workplace.

Long-term employees who have acquired considerable knowledge of an organisation's security procedures should be particularly monitored, as it is they who have the opportunity for fraud which exist and the influence to carry them out. Caution is also needed when internal disputes develop. A case heard before the New South Wales District Court on 27 March 1998, for example, concerned an unsuccessful applicant for a position with an Internet Service Provider (ISP). When he was refused the job he took revenge by illegally obtaining access to the company's database of credit card holders and publishing details relating to 1,225 cardholders on the Internet as a demonstration of the security weaknesses of the company. As a result, the business lost more than \$2 million and was forced to close its ISP activities.

Risks might also arise with the use of external contractors. As you move toward the implementation of on-line conveyance, you will need to rely heavily on contractors to develop, install and monitor new systems. Those individuals will have a detailed knowledge of the new systems and how to manipulate them. As such they may be subject to temptations to act illegally, particularly if disputes develop during the period of the contract. Particular care may be needed in ensuring that honest and trustworthy contractors are used in connection with secure systems.

### **3.7.4 Computer Usage Monitoring**

Employees' use of computers and their online activities can be monitored through the use of software which logs usage and allows managers to know, for example, whether staff has been using the Internet for non-work-related activities. Ideally, agreed procedures and rules should be established which enable staff to know precisely the extent to which computers are able to be used for private activities, if at all. If staff are permitted to make use of computers for private purposes, then procedures should be in place to protect privacy and confidentiality of communications, subject, of course, to employees obeying the law. Where certain online activities have been prohibited, it is possible to monitor the activities of staff, sometimes covertly such as through video surveillance or checking electronic mail and files transmitted through servers.

Filtering software may also be used to prevent staff from engaging in certain behaviours.

“Surfwatch”, for example, can be customised to deny employees access to specified content. When the employee requests a site, the software matches the user’s ID with the content allowable for the assigned category, then either loads the requested page, or advises the user that the request has been denied. The software also logs denied requests for later inspection by management.

The use of computer software to monitor business activities also provides an effective means of detecting fraud and deterring individuals from acting illegally.

### **3.8 The Consequences of Failure to Respond to Fraud within Organisations**

Where corporations have experienced electronic fraud, managers are faced with difficulty of choice. On the one hand, they may choose to “exit” the situation — and to dismiss the employee responsible, or cease doing business with the individual who perpetrated the offence. On the other hand, they may seek legal avenues of redress, either employing civil proceedings to recover compensation or criminal proceedings to punish the offender and to deter others from acting similarly.

Many organisations prefer not to report crime to the authorities. A survey of organisations through fraud conducted by Deakin University found that fraud was not reported officially because the matter was not considered to be serious enough to warrant police attention, a fear of consumer backlash, bad publicity, inadequate proof, and a reluctance to devote time and resources to prosecuting the matter. The reasons for the reluctance to report fraud are often due to a fear of “sending good money after bad” as experience may have shown that it will be impossible to recover losses successfully through legal avenues and that the time and resources which are required to report an incident officially and to assist in its prosecution simply do not justify the likely financial returns. Prosecution may entail countless interviews with the police, extensive analysis of financial records, and lengthy involvement in court hearings for staff.

The other disincentive to taking official action lies in the reluctance of organisations to publicise the fact of their victimisation through fear of losing business or damaging their commercial reputation in the marketplace. Government agencies might also believe that adverse publicity may result in a loss of confidence in voters, whilst financial institutions might believe that publicity of security weaknesses might

result in acts of repeat victimisation taking place using the same techniques as those being investigated.

Finally, where crime has been committed by those in positions of responsibility within organisations, they may not wish to draw undue attention to their own illegal activities. Although some of these responses are understandable, failure to take action creates an undesirable atmosphere in the organisation indicating that fraud is tolerated. It may also result in the offender in question being able to re-offend, either in the same organisation or elsewhere. Failure to report crime also means that new forms of crime do not receive publicity and thus others may be victimised in the same way. Finally, if crime is not reported then it is not possible to gather statistics on the nature and extent of incidents that take place. There are no easy fixes.

### **3.9 Recommendations**

Going back to the three opening points on what induces fraud, reducing fraud involves:

- Reducing the supply of motivated offenders
  - Protecting and educating the suitable targets
  - Limiting opportunities by making the crime more difficult to commit.
1. To deal with the first objective, reducing the supply of motivated offenders, is a hard one because there has always been greed, and the traditional crime prevention activities of early intervention are not applicable. People commit fraud without many of the usual risk or predictive factors. We are dealing here with culture and ethics - not something that comes in a five minute pep talk. It is here that things like effective corporate governance and ethical standards are central. At the other end of the spectrum, but dealing with the same issue of reducing the supply of motivated offenders, judicial punishments also play a role. Prison, which has few redeeming features, probably works better as a deterrent for fraud offenders than for many others. Similarly, confiscating a fraudster's home or car and requiring ill-gotten gains to be repaid over a lifetime are appropriate sanctions for white collar offenders.
  2. To deal with the second objective, protecting and educating the targets of fraud is a crucial part of the prevention equation. It involves imparting knowledge and information that will permit the identification of problems immediately they arise as well as a mechanism for keeping new information flowing, at both

individual and organisational levels. This goes hand in hand with a fraud control policy.

3. Limiting opportunities by making the crime more difficult to commit brings in the other side of the prevention equation, fraud control policies, computer usage monitoring, policing anomalies, corporate governance and professional regulatory procedures. The technologies of crime prevention are also of fundamental importance here. It all points to careful risk management. Risk management and fraud prevention are clearly preferable to the use of prosecution and punishment. Success in dealing with fraud will enhance Australia's business reputation, and reduce the personal hardship that fraud causes to countless victims each year.

Most fraud in the 21<sup>st</sup> century is sophisticated in planning and execution. Fraud prevention also needs to be sophisticated, although, as a recent British Home Office publication notes, it's "Not Rocket Science"! Some aspects of fraud prevention may involve us in taking basic measures to protect ourselves, such as by using the security measures that modern computing technologies have to offer in a sensible and thoughtful way—and not simply writing one's password on one's desk pad. Other target hardening measures may require elaborate and complex planning in order to thwart the efforts of fraudsters fully trained in the operation and management of electronic business systems. Managers also need to take personal responsibility for dealing with fraud and for reporting it to the authorities. This will not only help to inculcate an environment of honesty and openness within an organisation, but will enhance deterrent effects for other staff and enable the public generally to understand new areas of risk and security weaknesses. Sweeping fraud under the carpet by dismissing untrustworthy employees compounds the problem and creates an atmosphere of complacency within organisations. At every available opportunity, a **culture of compliance** needs to be reinforced.

In the end, fraud prevention and control require the concerted efforts of individuals working both within the public and private sectors who make use of the most up-to-date and effective fraud control technologies. When all else fails, an efficient legal system must also exist to detect, investigate, adjudicate, and sanction those who seek to obtain funds dishonestly. There has been considerable progress in each of these aspects already and Australia is at the forefront of many innovative developments in fraud control. The challenge for the years to come lies in understanding how new forms of fraud are perpetrated and ensuring that those charged with preventing and dealing with fraud have adequate resources to do their work. Although the systems being introduced to facilitate electronic land transactions will entail much

efficiency, they will also, unwittingly, create new opportunities for crime. As in most areas of crime control, it is better to allocate resources in preventing crime than in seeking to deal with the consequences after the problem has arisen.

#### **4.0 CONCLUSION**

Fraud is not going to go away. The electronic systems used to conduct commercial transactions are changing rapidly, and considerable effort is being put into ensuring the security of digital transmissions which represent monetary value. The opportunities for fraud are, however, substantial. The solution to electronic fraud will ultimately involve the adoption of a range of strategies which will be both technological and strategic in which close cooperation will exist between all those involved in providing and using systems. This includes telecommunications carriers and service providers, financial institutions, corporations, and individual users.

#### **5.0 SUMMARY**

- Fraud involves the use of dishonest or deceitful conduct in order to obtain some unjust advantage over someone else.
- The circumstances in which fraud can exist are enormously diverse. Some of the types include: commercial fraud, fraud against governments, consumer fraud, migration fraud, securities fraud, superannuation fraud, intellectual property fraud, computer and telecommunications fraud, insurance fraud, plastic card fraud, art fraud, charitable contribution fraud, identity-related fraud, advance fee fraud, health care fraud, and the list goes on and on, and new opportunities for deceptive conduct arise all the time.
- The techniques that have been used to commit fraud in these areas are exactly the same as those that could be used to attack the Offices of Titles around Australia.
- All companies and organisations move money electronically. In the olden days, law clerks would stand in line at the Titles Office and hand a piece of paper over to an officer at the counter who probably knew the person by sight, and if there was an anomaly, it would be picked up by the official who just knew!
- In the olden days bushrangers and outlaws used masks to cover their faces so nobody would know who they were. Today, on the Internet, nobody really knows who you are.
- An illustration of the risks that online service delivery can entail is electronic share trading. The use of computers and e-mail has greatly facilitated the manipulation of share markets during secondary trading of securities. These are only some of the types of fraud facing Australian organisation today.

- It is important for those who manage organisations to have a proper understanding of the risks that are present within their organisations.
- There is also a need for organisations to be confident that the staffs they are employing are reliable and trustworthy, as electronic fraud often involves confederates with inside knowledge of a company's security and computer procedures.
- Employees' use of computers and their online activities can be monitored through the use of software which logs usage and allows managers to know, for example, whether staffs have been using the Internet for non-work-related activities.
- Where corporations have experienced electronic fraud, managers are faced with difficult choices as to how they should respond
- Most fraud in the 21<sup>st</sup> century is sophisticated in planning and execution.
- Fraud prevention also needs to be sophisticated.

## **6.0 TUTOR-MARKED ASSIGNMENT**

1. Identify general factors that lead to fraud and the 3 ways to limit fraud.
2. What are some of the consequences of not responding to fraud in an organisation?

## **7.0 REFERENCES/FURTHER READINGS**

Adam Graycar & Russell Smith, "Identifying and Responding to Electronic Fraud Risks". Australian Institute of Criminology, 30<sup>th</sup> Australasian Registrars' Conference Canberra November 13, 2002.