



Ethical Hacking and Countermeasures

Version 6



Module LVIII

Credit Card Frauds

Three Indicted on Fraud Charges

Posted: Feb 20, 2008 12:22 AM

Updated: Feb 20, 2008 12:22 AM

From the US District Attorney's Office, District of South Carolina:

COLUMBIA, SC - United States Attorney Reginald I. Lloyd stated that a Federal Grand Jury indicted Mary Daniels, age 25, of Waverly, Georgia, James Driggers, age 23, of Bluffton, South Carolina, and Amanda Tuyls, age 25, of Hardeeville, South Carolina, for mail theft, identity theft, and credit card fraud.

Count one of the indictment alleges that from August 2007 through October 2007, Daniels and Driggers stole mail from residential mail boxes. Count two alleges that from August 2007 through October 2007, Daniels, Driggers, and Tuyls committed more than \$1,000 in credit card fraud. Count three alleges that from August 2007 through October 2007, Daniels and Driggers possessed and used, without lawful authority, another person's name and address to commit a federal crime. Count 4 alleges that on September 12, 2007, Daniels used, without lawful authority, another person's name and address to commit bank fraud.

The maximum penalty that Mary Daniels and James Driggers could receive is a fine of \$250,000 and imprisonment of 15 years, while the maximum penalty that Amanda Tuyls could receive is a fine of \$250,000 and imprisonment of 10 years.

The case was investigated by agents of the Postal Inspection Service and the Hardeeville Police Department and has been assigned to Assistant United States Attorney Rhett DeHart of the Charleston office for prosecution.

The United States Attorney stated that all charges in this Indictment are merely accusations and that all defendants are presumed innocent until and unless proven guilty.

Source: <http://www.wtoctv.com/>

BRANDY'S MOM ACCUSES KARDASHIAN OF CREDIT CARD FRAUD



REUTERS/Fred Prouser (UNITED STATES)

The mother of R&B star Brandy has accused socialite Kim Kardashian of committing credit card fraud.

Sonja Norwood filed a lawsuit in L.A. County Superior Court on Monday against the star, after Kardashian allegedly abused the use of a credit card given to her to make "one (and only one)" purchase on behalf of Norwood.

However, Kardashian is accused of giving the American Express card to other members of her family, Khloe, Kourtney and Robert Jr. The three are alleged to have run up debts of \$120,635 on the card in 2006 and 2007.

The suit also claims thousands of dollars from the unauthorized payments were charged in the family's Dash and Smooch stores, reports TMZ.com.

Kim Kardashian has dismissed credit card fraud claims against her as "meritless."

Kardashian, who famously dated Brandy's brother Ray J and appeared in a sex tape with him, insists she is innocent.

Her spokesperson says, "The charges against the Kardashians are meritless. Both Kim and Khloe were employed by the Norwoods and never used their credit cards without their express authorization.

Source: <http://www.sfgate.com/>

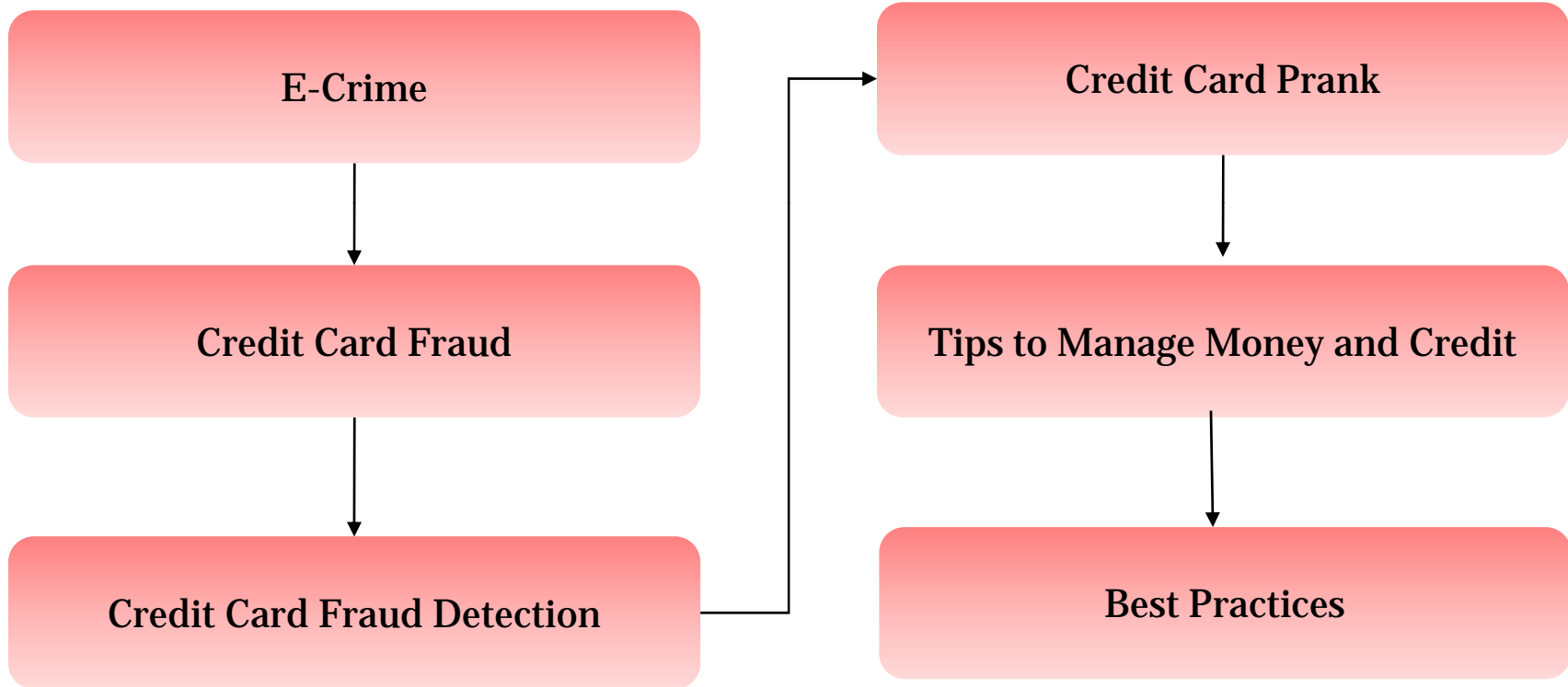
Module Objectives

This module will familiarize you with:

- E-Crime
- Credit Card Fraud
- Credit Card Generator
- Credit Card Fraud Detection
- Credit Card Prank
- Tips to Manage Money and Credit
- Best Practices



Module Flow



E-crime is when a computer or other electronic communications devices (e.g. mobile phones) are used to commit an offence; be it the target of an offence or act as a storage device in an offence

Source: <http://www.netalert.gov.au/>

Common offences committed via E-Crime:

- Credit Card Fraud
- Online auction fraud
- Computer Hacking
- Forwarding of Offensive/Menacing or Harassing Emails

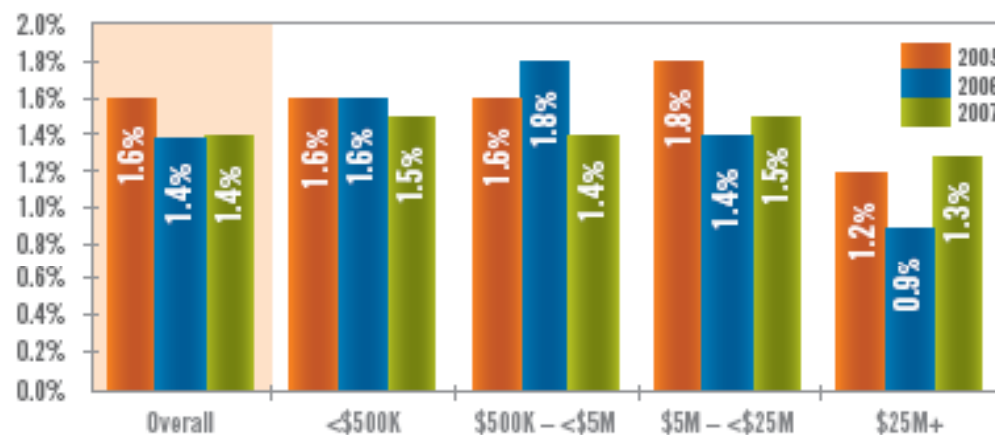




2007

Source: <http://www.idssafety.net/>

Average % Online Revenue Lost to Payment Fraud
(Chargebacks & Fraud-Related Credits)



Annual Online Revenues

2008

Source: <http://www.cybersource.com>

Credit Card



Source: <http://i197.photobucket.com/>



Credit Card Fraud

Case Study

Credit card fraud

Mr R ran a crash repair and spare parts business. His father was the director of the company that had previously owned the business and continued to assist Mr R with the bookkeeping for Mr R's company which had taken over the business.

In March 2005, two customers purchased items from the business and paid by credit card. In April, Mr R's bank wrote to him asking him to produce the credit card sales vouchers because the credit card owners said that the use of their credit cards was unauthorised and they disputed that they had purchased goods from the business. Mr R had 10 days to provide the vouchers.

As Mr R's father was away on holidays at the time the bank's letters arrived, Mr R did not open the letters from the bank. There were telephone conversations between the bank and Mr R about the provision of the sales vouchers and they were eventually provided to the bank in June 2005. The bank said that it was then too late to produce the sales vouchers and that under the terms of the merchant agreement the business was liable for the disputed transactions. Transactions totalling \$3,800 were charged back to Mr R's company's account.

Dispute

On behalf of Mr R's company, Mr R's father argued that the bank was not entitled to charge back the transactions to the business account and could not rely on the terms of the merchant agreement that the bank referred to. He argued that the only merchant agreement was the original merchant agreement between the bank and his company which did not bind the company for which Mr R was the director. He also said that the bank had given Mr R an extension of time to produce the sales vouchers and then told Mr R that it was not necessary to provide copies of the sales vouchers.

The bank provided copies of diary notes of the conversations between it and Mr R and said that it had not misled Mr R about extending the time for providing vouchers or about the need to provide vouchers. It said that the merchant agreement was an enforceable contract between the bank and Mr R's company because since 2002 Mr R's company operated as if the merchant agreement was in place and in 2003 Mr R's father signed a merchant variation agreement agreeing to be bound by the merchant agreement originally established in 1997.

Source: <http://www.bfso.org.au/>

Case Study

Identity theft case study 2 - Auto loan reveals credit card fraud

An elderly member contacted Kroll's Fraud Solutions upon being notified by local police that a **suspect in custody had been using his identity**. The suspect was part of a car theft ring, and had been apprehended in a sting operation. The crooks had purchased the victim's personal identifying information from a local merchant where the victim had previously conducted business.

The victim was very upset and overwhelmed. After counseling him and explaining the steps involved, his **Fraud Solutions Licensed Investigator called the police** for more details of the crime as well as a copy of the police report. We also sent one of our fraud restoration packets to the victim.

Upon receiving the member's necessary documents for restoration, the victim's Licensed Investigator immediately placed fraud alerts, and notified Social Security, the FTC, and the US Postal Inspector. A copy of the victim's 3 bureau merged credit report was also ordered and sent to him directly. Upon receipt of the credit report, the **victim discovered two open, fraudulent credit card accounts in addition to the falsified automobile loan**.

Fraud Solutions began its process of disputing the fraudulent accounts on the victim's behalf. The victim's local police department had already contacted the bank that financed the car. The Fraud Solutions investigator still followed up with the bank, until the issue was resolved and the **victim received written confirmation** that he had been absolved of all financial responsibilities.

Kroll contacted the two credit card companies involved and sent detailed dispute letters to their respective fraud departments, requesting that the fraudulent accounts be deleted from the victim's credit history. The **credit card companies acknowledged the fraud**, responded to Kroll's dispute letters within the allotted period provided in the Fair Credit Reporting Act (FCRA). In addition, pursuant to the FCRA, the credit card companies stated that they would remove all fraudulent accounts and inquiries from the victim's credit history.

Source: <http://www.krollfraudsolutions.com/>

Credit Card Fraud

Credit card fraud is a theft and fraud carried out using a credit card or any alike payment mechanism as a fake source for fund transaction

Common type of credit card fraud happens when an offender purchases an item online or by telephone, by utilizing a credit card number that they have obtained unlawfully

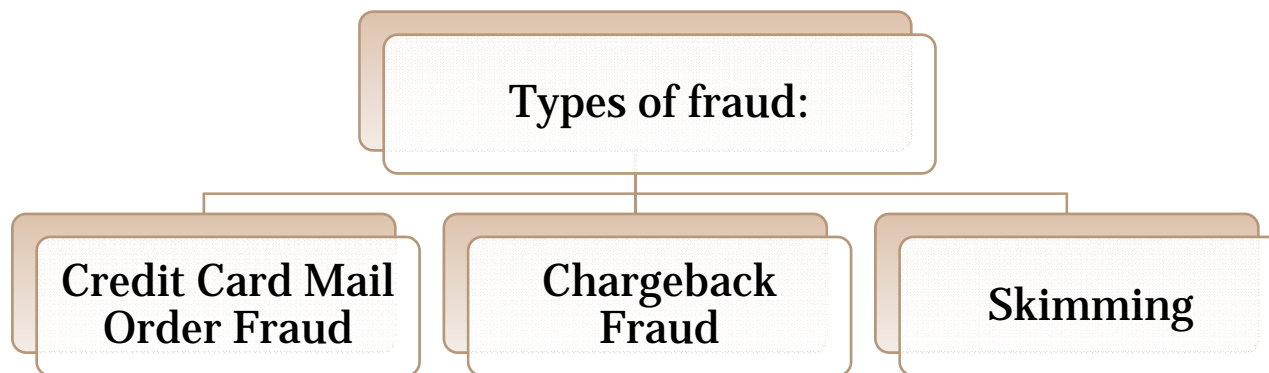
These numbers can be obtained from:

- A credit card generator site on the Internet
- An unscrupulous retail merchant retaining credit card numbers processed through a retail outlet and using them unlawfully
- Offenders who utilize skimming machines to record multiple credit card numbers via retail outlets
- Sourcing discarded copies of credit card vouchers via waste receptacles
- Hacking into computers where credit card numbers are stored

Credit Card Fraud Over Internet

Credit Card Fraud Over Internet is a term used for unauthorized and illegal use of a credit card to purchase property over the Internet

The fraudster uses the credit card or debit card of another person for transaction



Net Credit/Debit Card Fraud In The US After Gross Charge-Offs

Net Credit/Debit Card Fraud In The US After Gross Charge-Offs

| Year | All Cards (in millions) | Bank Cards (in millions) |
|------|-------------------------|--------------------------|
| 2004 | 1,652.48 | 1,164.96 |
| 2005 | 1,817.68 | 1,294.09 |
| 2006 | 1,991.96 | 1,429.68 |
| 2007 | 2,183.70 | 1,580.86 |
| 2008 | 2,392.40 | 1,745.45 |
| 2009 | 2,623.31 | 1,927.38 |
| 2010 | 2,877.21 | 2,127.87 |

Estimated US Online Credit Card Fraud, 2003 - 2007

| Year | USD billion |
|------|-------------|
| 2003 | 2.3 |
| 2004 | 2.6 |
| 2005 | 2.7 |
| 2006 | 3.0 |
| 2007 | 3.2 |



Credit Card Generators

Credit Card Generator

www.darkcoding.net

Credit Card Generator is a command line Python program which uses PHP script and JavaScript

It generates credit card numbers that are used to test e-commerce sites

It generates 13 and 16 digit VISA, MasterCard, and Amex numbers

If installed, it can steal passwords, credit card numbers, and bank details




RockLegend's !Credit Card Generator

RockLegend's !Credit Card Generator Generates/Validates Credit card Numbers

RockLegend's Cool

Credit Card Number Checker/Generator

Read the [disclaimer](#) first

| | | |
|--|----------------------|----------|
| Number | <input type="text"/> | Check |
| | Discover | |
| Number | 60xx xxxx xxxx xxxx | Generate |
|  | | |

This program generates and validates credit card numbers. Card holder's name and expiration date are not coded into the card number, thus any name and expiration date can fit any valid number. To check to see if a number is valid, type it into the box next to check and click the "check" button. To generate a credit card number, pick a credit card format and click generate.




Credit Wizard

www.creditcardgenerator.org

Credit Wizard v1.1 - b1

Credit

Card



☒ Visa ☐ MasterCard ☐ Discover

Info Generator

First name: Last name:

Address:

City: St. Zip:

Phone: -

Numbers:

Banks:

4013 - Citibank

4019 - Bank of America

4024 - Bank of America

4027 - Rockwell Federal Credit Union

4032 - Household Bank

4052 - First Cincinnati

4060 - Associates National Bank

4070 - Security Pacific

4071 - Colonial National Bank

4094 - A.M.C. Federal Credit Union

4113 - Valley National Bank

4114 - Chemical Bank

Bank Prefix:

Number of cards:

Credit Wizard 1.1



Credit Card Fraud Detection

Anatomy of an Internet Credit-Card Scam

They're an unlikely set of adversaries. Daniel Vasiliu, a teenager from Bucharest, Romania and David Stien, a middle-aged credit union manager from Indiana. Here's how the winds of global Internet fraud likely brought the two together.

1. Vasiliu gets valid credit-card accounts by using a credit-card number generator freely available on the Net. (All card numbers are based on an underlying algorithm originally designed to prevent key-punch errors by store clerks. The generator, a software program, simply creates a number using that algorithm, making it easy to come up with a legit account.) The card numbers happen to use Crane Federal Credit Union's bank identification number.
2. Vasiliu tests the validity of the card numbers by buying memberships at sex sites on the Web.
3. With valid card numbers in hand, Vasiliu goes on a shopping spree. He proceeds to e-commerce sites--such as FTD and tiny Colorado computer reseller LEM Computers--and orders goods sent to Romanian addresses.
4. Merchants confirm the validity of orders. The scam is made easier because there is no address-verification service for foreign credit-card orders. In the U.S., address verification is another safety net for merchants, matching delivery information to card-holder information on file. Such a system would have red-flagged the Vasiliu order.
5. Vasiliu starts receiving merchandise--watches, flowers, cigars, computer products-- while Crane members start receiving the bills.

<http://www.businessweek.com/>

Credit Card Fraud Detection

Technique: Pattern Detection

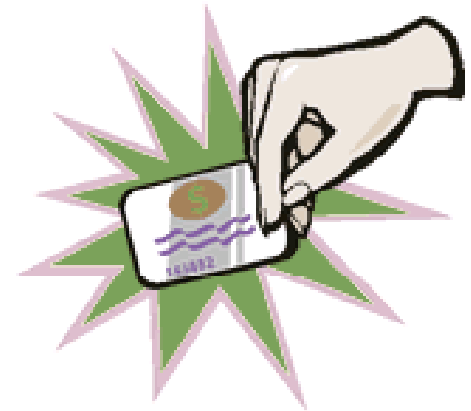
This technique identifies a person as a fraudster if:

Multiple orders are placed which are to be delivered to the same address, but using different credit cards

Multiple orders are being sent from the same IP address

The credit card number varies by only a few digits

User repeatedly submits same credit card number with different expiry dates



Credit Card Fraud Detection Technique: Fraud Screening

It is a part of CyberSource Decision Manager

This technology is enhanced by Visa, which provides fraud risk prediction scores by assessing over 150 order variables

These order variables include domestic and international address validation, and domestic and international IP address verification



Credit Card Fraud Detection

Technique: Fraud Screening (cont'd)

Features:

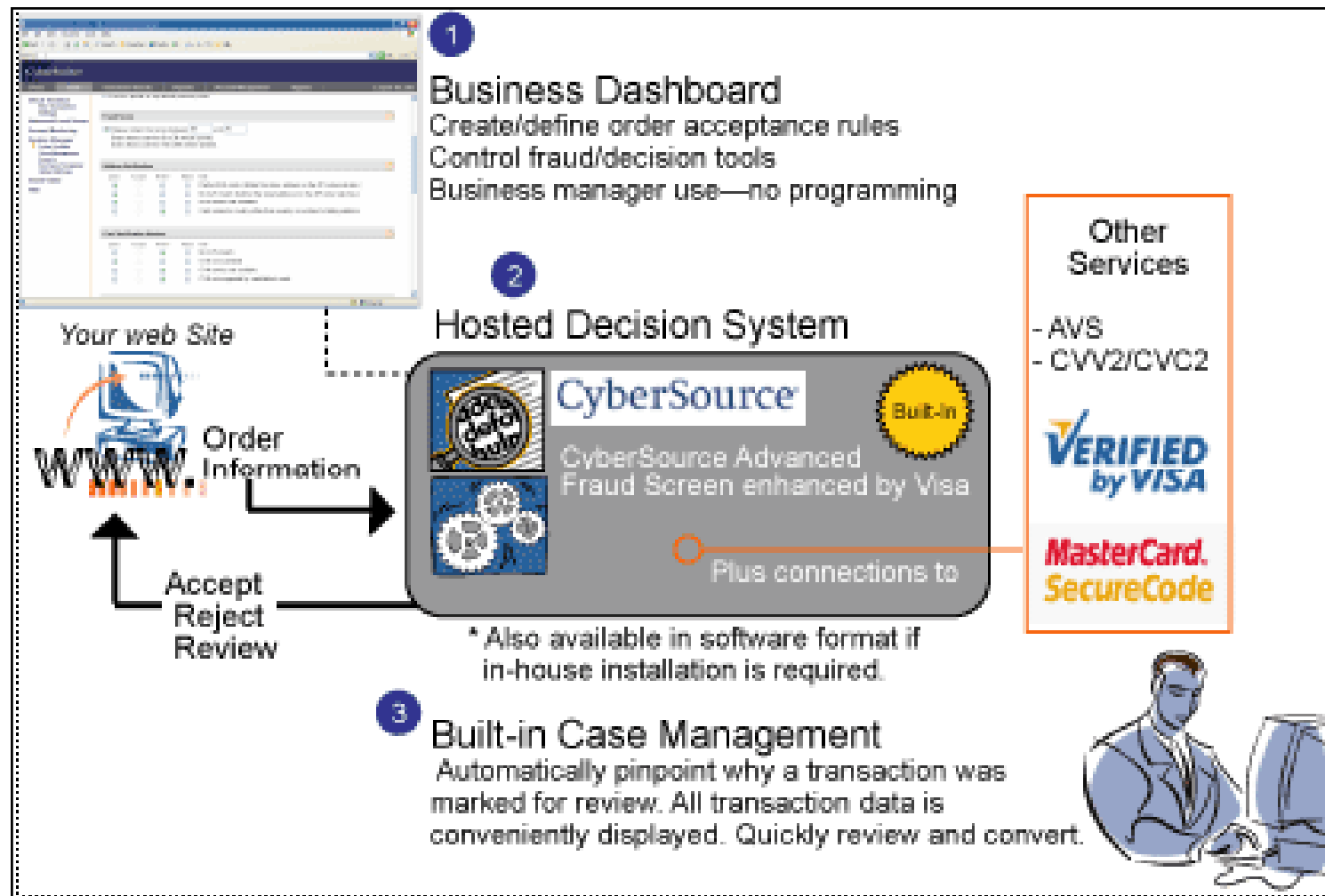
- Shown to control fraud to as little as 0.5%
- Automatically identifies whether an order is valid or potentially fraudulent in real time
- Patented global identity morphing detection
- Detailed, web-based reports

Benefits:

- Detects more single-event fraud as soon as it occurs
- Detects fraud trends more quickly
- Minimizes time, cost of manual review



Fraud Screening: Screenshot





XCART: Online fraud Screening Service

[Shopping carts](#) [Ecommerce solutions](#) [Software for online shops](#)

[Home](#) [Site map](#)



PRODUCTS

SERVICES

DEMOS

BUY

CONTACT

SUPPORT

ALLIANCES

[Home page](#) :: [Online fraud screening service](#)

Custom development

Web design

X-Cart hosting

Holiday decoration

Turn-key installation

Online fraud screening

Online fraud screening service

For better merchant protection from online credit card fraud X-Cart 4.0 has an integrated fraud screening facility. Antifraud service is a subscription based service; however with X-Cart license we offer a free trial for antifraud screening.

If fraud screening is enabled, X-Cart transfers non personal data about a placed order to our antifraud service, where the request is processed and estimated risk factor for the order is returned. If risk factor exceeds the specified threshold then the order is delayed for manual check (phone call to a buyer, asking for additional evidence of authenticity etc.). Antifraud system provides a detailed report with an explanation what was suspicious about the order. This functionality is particularly useful when selling goods with immediate electronic delivery (like software, music, content etc.) because this kind of goods are most often ordered using stolen credit cards.

We are utilizing MaxMind's GeoIP/minFraud service for Antifraud service. GeoIP databases are 99% accurate on a country level, 85% accurate on a state level, and 80% accurate for the US within a 25 mile radius. But the risk factor is assessed by our unique algorithms based on our substantial experience in online credit card processing and which are specially adapted to be used in X-Cart shopping cart system. No sensitive private customer's information (like name, email address, CC numbers) is sent to our screening servers during antifraud checks.

To use this service, please open "Buy products/services" page in your [HelpDesk](#) account and purchase "Antifraud Service subscription (10 000 requests a year)". Upon the purchase a key is provided. This key is to be used on Antifraud service page of your installation of X-Cart. Please refer to the [user manual](#) for a better description.

One key can be used in up to 4 stores. if a request from 5th store comes, antifraud service becomes unavailable for the store which has not been requesting the service for the longest time among the other 4.

However, if within a year time since the purchase the subscription is extended by acquiring another set of 10 000 requests, the remaining requests of the older key will be added to the new ones, so you will have 10000 extra requests together with the remaining from the older purchase.

Card Watch is a UK banking industry initiative that aims to raise awareness of card fraud prevention

It is managed by APACS, the UK payments association

The Card Watch prevents credit card fraud by:

- Providing fraud prevention training for retail staff through retailer training programs and publications, including the Spot & Stop Card Fraud training materials
- Encouraging staff vigilance and awareness to aid in the prevention of card crime
- Providing fraud prevention advice for cardholders
- Providing education and support to police and crime reduction officers
- Giving advice and assistance to other fraud prevention organizations such as Crime stoppers
- Running an annual card security initiative to increase awareness amongst the public and other relevant stakeholders



SPOT AND STOP CARD FRAUD

interactive training

help!



welcome to cardwatch spot and stop
card fraud interactive training site

Learn more about Card Fraud and how to prevent it – log in, read and understand the modules then complete the tests. A certificate will be issued if you pass.

> log in

[Registered Users](#)

[Public Users](#)



MaxMind Credit Card Fraud Detection

MaxMind's minFraud is a leading cross-industry and cross-platform fraud detection solution powered by various in-house developed proprietary technologies

It analyzes and scores risk factors for each online transaction in real-time so that merchants can make better informed decisions, process more orders with less staff, and reduce the amount of time spent on manual review

The minFraud service works in the background without the customer's knowledge and does not require the customer to go through extra steps during the checkout process

For example, if MaxMind detects suspicious activity from an IP address, it will be flagged throughout the network in real-time, allowing for a more dynamic and adaptive approach to fraud detection

MaxMind Credit Card Fraud Detection (cont'd)

Key Benefits

- Reduces chargebacks, losses from fraudulent orders, and fraud attempts
- Mitigates the risks of selling cards worldwide where conventional card-authorization tools may not be available
- Saves on gateway and processing fees by filtering out fraudulent orders
- Adds fraud detection capabilities for alternative payments like PayPal and ACH

Key features

- Geographical IP address location checking
- High risk IP address and e-mail checking
- Issuing bank BIN Number country matching minFraud Network
- Post query analysis





Support



My Account



FAQ



My Order

Home

GeoIP

minFraud

Contact

Company

What is minFraud?

Success Stories

Feature Comparison

Integration

Trial Account

Buy Now

Support Center

Reduce Credit Card Fraud with minFraud

Fraudster techniques becoming more advanced

Techniques used in online card-not-present fraud are becoming more and more sophisticated. Traditional fraud screening tools can only determine if a credit card is legitimate or if the user-entered account information matches those on record. Today, fraudsters can obtain personal credit card information, pose as the legitimate card holder, and bypass standard fraud checks.

Looking at fraud from a different angle

At MaxMind, we approach fraud screening in a different way. We examine an online transaction from various angles. Our tools are not geared towards verifying the authenticity of the credit card details used for the purchase, but rather, identifying if the purchaser is the legitimate card holder. Through our analysis, we have been able to identify traits and patterns that are associated with fraudulent orders. By asking the right questions, we can provide e-commerce businesses with the necessary information to detect fraudulent orders before the payment is processed.

Key features include: ([Download](#) MaxMind minFraud White Paper)

- Geographical IP address location checking
- High risk IP address and e-mail checking
- Issuing bank BIN Number country matching
- minFraud Network
- Post query analysis
- Cost-effective pricing starting at \$0.004 per transaction

➤ For added protection, use minFraud in conjunction with our [Telephone Verification Service](#)

3D Secure authentication requires cardholders to register their card to take advantage of this service

It is a one time process which takes place on the card issuer's website and involves the cardholder answering several security questions to which only the card issuer and the cardholder have the answer

3D Secure can be thought of as an online version of 'Chip and Pin' technology, whereby the cardholder has a personalized password registered with his/her card that is entered during the checkout process



Limitations of 3D Secure

3D Secure authentication should not be used as a complete fraud prevention tool, but should be used in conjunction with existing fraud checks such as AVS and CVV2 to help minimize your risk of fraud

Chargebacks can still occur even when they have been fully authenticated by 3D Secure



FraudLabs is an XML-based service that validates online credit card transactions

FraudLab's web service screens and detects online credit card fraud

FraudLabs is a proven solution to prevent chargebacks and reduce fraud for online merchants



Screenshot 1

Fraud Labs Web Service - <http://www.fraudlabs.com>

FRAUDLABS
Preventing Online Fraud

Free License Subscribe About Exit

Web Service

| | | | | | |
|-------------|-----------|--------------|-------------|------------------|----------|
| IP Address | 200.0.0.1 | Phone No | 604-5566543 | Ship Region | |
| City | | BIN | | Ship Postal Code | 13456 |
| Region | | BIN Name | | Ship Country | COLOMBIA |
| Postal Code | 13456 | BIN Phone No | | Query ID | 12345 |
| Country | COLOMBIA | Ship Address | | License Key | |
| Domain | gmail.com | Ship City | New York | | |

Process Clear

Results

| | | | | | |
|-------------------|-----|-------------------|-----------|-------------------|----------|
| Anonymous Proxy | NO | Credits Available | 99943 | IP to Latitude | 4.6 |
| BIN Bank Name | | Distance | 0 | IP to Longitude | -74.0833 |
| BIN Bank Phone | | Fraud Score | 44 | IP to Region | . |
| BIN Country | | Free Email | YES | Message | |
| BIN Country Match | | High Risk Country | YES | Phone City Match | |
| BIN Name Match | | IP to City: | . | Postal City Match | |
| BIN Phone Match | | IP to Country | COLOMBIA | Query ID | 12345 |
| Country | CO | IP to ISP | HOCOL S.A | Ship Forward | |
| Country Match | YES | | | | |

Screenshot 2

STEP 1: INPUT QUERY

Demo Instruction:

1. Fill in the fields in the boxes shown below.
2. Press the "Submit" button.

| | |
|------------------|------------------------------|
| IP Address | 68.142.197.65 |
| City | SAN MATEO |
| Region | CALIFORNIA |
| Postal | 00501 |
| Country | US |
| Email Domain | webmaster@hotmail.com |
| Phone | 6041111111 |
| BIN | 541726 |
| BIN Name | SOUTHERN BANK BERHAD |
| BIN Phone | 60362047878 |
| Shipping Address | BLOCK D2 515-c, LORONG TUNA, |
| Shipping City | PRAI |
| Shipping Region | PENANG |
| Shipping Postal | 13700 |
| Shipping Country | MALAYSIA |
| Query ID | 00000 |

Clear Screen

Submit

FraudLabs.com allows maximum 20 lookups per IP address per day.
You have 19 lookup credit(s) today.

Screenshot 3

STEP 2: ANALYZE AND PROCESS OF QUERY

```
<HIGHRISKCOUNTRY>NO</HIGHRISKCOUNTRY>
<DISTANCE>33</DISTANCE>
<IP2COUNTRY>US</IP2COUNTRY>
<IP2REGION>CALIFORNIA</IP2REGION>
<IP2CITY>SUNNYVALE</IP2CITY>
<IP2LATITUDE>37.3779</IP2LATITUDE>
<IP2LONGITUDE>-122.027</IP2LONGITUDE>
<IP2ISP>INKTOMI CORPORATION</IP2ISP>
<ANONYMOUSPROXY>NO</ANONYMOUSPROXY>
<FREEMAIL>YES</FREEMAIL>
<BINCOUNTRYMATCH>NO</BINCOUNTRYMATCH>
<BINNAMEMATCH>YES</BINNAMEMATCH>
<BINPHONEMATCH>YES</BINPHONEMATCH>
<BINCOUNTRY>MY</BINCOUNTRY>
<BINBANKNAME>SOUTHERN BANK BERHAD</BINBANKNAME>
<BINBANKPHONE>60362047878</BINBANKPHONE>
<POSTALCITYMATCH>NO</POSTALCITYMATCH>
<PHONECITYMATCH>NO</PHONECITYMATCH>
<SHIPFORWARD>NO</SHIPFORWARD>
<FRAUDSCORE>29</FRAUDSCORE>
<QUERYID>00000</QUERYID>
</FRAUDLABS>
```

STEP 3: RETURN RESULTS

Results:

```
Anonymous Proxy : NO
BIN Bank Name : SOUTHERN BANK BERHAD
BIN Bank Phone : 60362047878
BIN Country : MALAYSIA
BIN Country Match : NO
BIN Name Match : YES
BIN Phone Match : YES
Country : US
Country Match : YES
Distance : 33
Fraud Score : 29
Free Email : YES
High Risk Country : NO
IP to City : SUNNYVALE
IP to ISP : UNITED STATES
IP to Latitude : INKTOMI CORPORATION
IP to Longitude : 37.3779
Phone City Match : -122.027
IP to Region : CALIFORNIA
Phone City Match : NO
Postal City Match : NO
Query ID : 00000
Ship Forward : NO
```



- > [Company](#)
- > [Services](#)
- > [Pago Partner Program](#)
- > [Market & Trends](#)
- > [Press Room](#)
- > [Shop](#)
- > [Support](#)



Pago AVS

Address verification for online shoppers from the USA.

[» Pago AVS](#)



[Home](#) - [Services](#) - [Risk Management Services](#) - [Pago Fraud Screening](#)

Better play it safe



Credit card fraud is a threat to your business. If you don't get paid for your goods, you incur multiple losses. E-Commerce has become a playground for organized crime and their illegal activities. Therefore, tools for fraud prevention are a must for each and every online merchant.

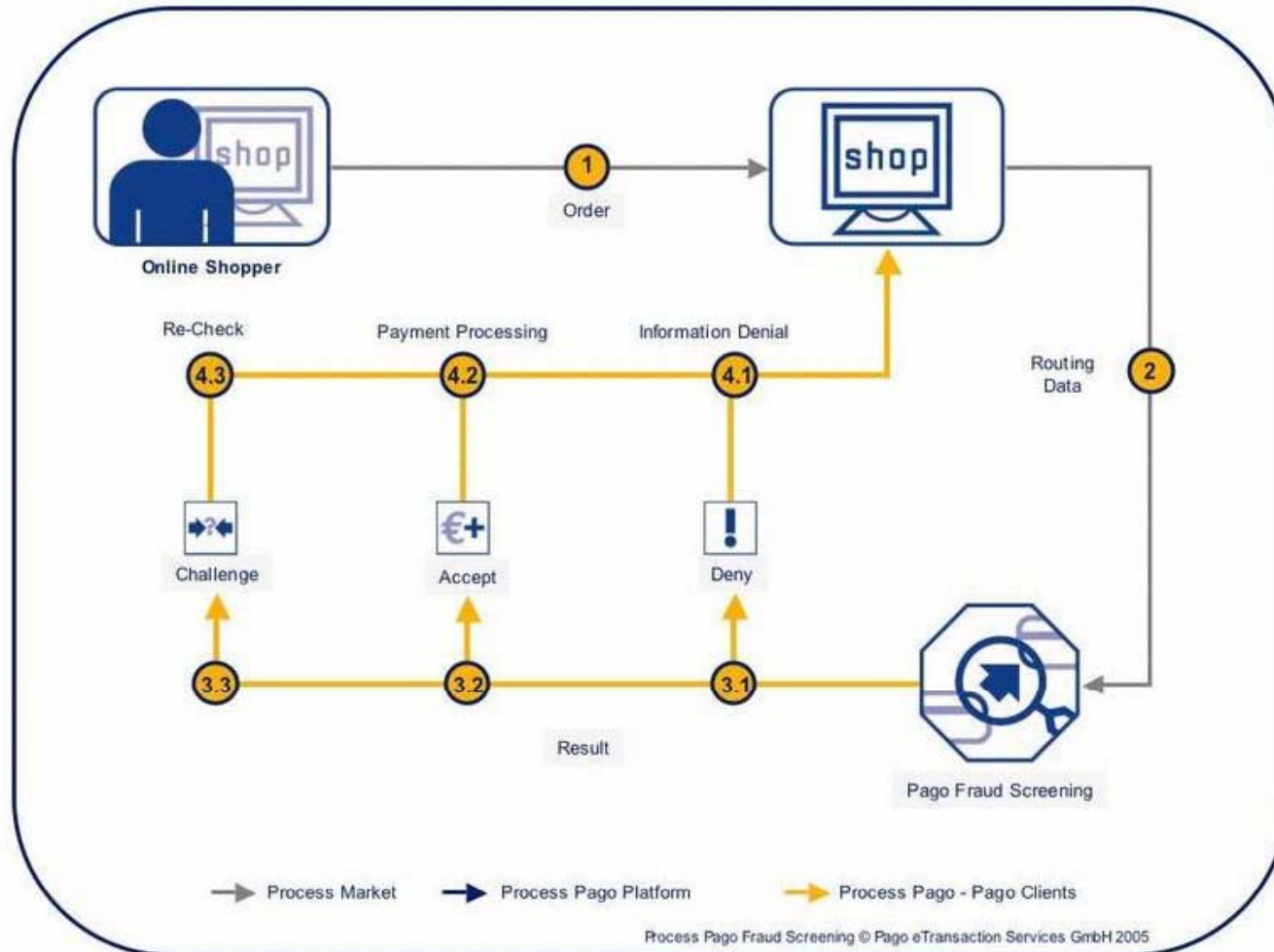
Pago Fraud Screening is the ideal security service for efficient protection against credit card fraud.



Overview

- [The principle of Pago Fraud Screening](#)
- [Pago Fraud Screening FAQ](#)
- [Additional Risk Management Services](#)

Pago Fraud Screening Process





U.S. Department of Justice
United States Attorney
Northern District of Ohio
Gregory White
Robert W. Kern
Assistant U.S. Attorney
(216) 622-3836

Parma, Ohio Man Indicted for Ebay Fraud, Credit Card Fraud, and Identity Theft

Gregory A. White, United States Attorney for the Northern District of Ohio, announced today that a federal grand jury in Cleveland, Ohio, returned a forty-five count indictment charging Jeffrey P. Butcher, age 43, of 7509 Kenilworth Avenue, Parma, Ohio, with forty-three counts of wire fraud, in violation of Title 18, United States Code, Section 1343, one count of identity theft, in violation of Title 18, United States Code, Section 1028(a)(7) and one count of credit card fraud, in violation of 18 U.S.C. § 1029(a)(5). Counts 1 through 43 of the indictment charge that between March 11, 2003, and May 1, 2003, the defendant transmitted and caused the transmission of interstate wire communications for the purpose of executing a scheme to defraud bidders on Ebay, an internet auction website. The indictment charges that Butcher advertised computer equipment, including Pentium computer chips, for sale on Ebay, received payments from individuals for items sold on Ebay, but failed to provide the items to forty-three individual purchasers. The indictment charges that as a result of this scheme and artifice, Butcher caused losses totaling approximately \$30,653.76.

Count 44 (identity theft) charges that between December 1, 2003, and December 31, 2003, Butcher applied for 10 credit card accounts using the identifier information of Dureene Kiplinger, including her name, social security account number and date of birth, without authorization.

Count 45 (credit card fraud) charges that between December 1, 2003, and December 29, 2003, Butcher knowingly, and with the intent to defraud, obtained and used a Home Depot credit card issued in the name of Dureene Kiplinger, thereby obtaining goods and services valued at approximately \$7,742.44. The statutory maximum sentence for each violation of Title 18, United States Code, Section 1343 is 20 years in prison, a fine of up to \$250,000, or both. The statutory maximum sentence for a violation of Title 18, United States Code, Section 1028(a)(7) is 15 years in prison, a fine of up to \$250,000, or both. The statutory maximum sentence for a violation of Title 18, United States Code,

<http://www.usdoj.gov/criminal/cybercrime/butcherIndict.htm>

What to do if you are a Victim of a Fraud

When you use a credit card, you can be vulnerable to fraud, whether you pay online, over the phone, or even in person at your neighborhood grocery store

If you think you have been the victim of fraud or a scam, immediately follow these steps:

- Close any affected accounts
- Change the passwords on all your online accounts
- Place a fraud alert on your credit reports
- Contact the proper authorities
- Record and save everything

Facts to be Noted by Consumers

A thief goes through trash to find discarded receipts or carbons, and then uses your account numbers illegally

A dishonest clerk makes an extra imprint from your credit or charge card and uses it to make personal charges

You respond to a mail asking you to call a long distance number for a free trip or bargain-priced travel package. You are told you must join a travel club first and you are asked for your account number so you can be billed. The catch! Charges you did not make are added to your bill, and you never get your trip

Credit Card Fraud Earns Man 13 Years In Prison - No Fun Says Business Ethics Speaker Chuck Gallagher



Peter Porcelli II, age 55, will now get to serve 13 years (or almost one-fourth of his life thus far) in prison for credit card fraud. Wonder now if he feels that his ill gotten gains are worth it?

The Associated Press article printed in the International Herald Tribune is reprinted as follows:

A man accused of orchestrating a scheme to sell bogus credit cards was sentenced to 13 years in prison and must repay the nearly \$12 million (€8.3 million) he scammed from tens of thousands of U.S. customers.

Peter Porcelli II, 55, who lives in Florida, pleaded guilty in May to all 19 conspiracy and fraud counts related to the telemarketing scheme. U.S. District Judge William Stiehl also ordered Monday that he spend five years on supervised release after his prison term.

Prosecutors alleged Porcelli offered consumers a MasterCard credit card for a fee ranging from \$160 (€111) to \$500 (€347). Those charged the fee were sent offers that usually were already available for free to the public, along with an "acceptance form" for what amounted to a prepaid card, which cost consumers an extra \$15 (€10.41).

Authorities say Porcelli defrauded or tried to dupe at least 165,000 Americans, many with poor credit histories.

The U.S. government alleged that Porcelli carried out the scam through several Florida-based companies beginning in June 2001, using call centers in several states and outside the U.S.

Porcelli has been free on \$1 million unsecured bond since shortly after his federal indictment in March.

Source: <http://chuckgallagher.wordpress.com>

Copyright © by **EC-Council**



Best Practices

Best Practices: Ways to Protect Your Credit Cards

Sign your cards as soon as they arrive

Never leave credit cards unattended

Protect your Personal Identification Number (PIN) or security code

Check your card when returned to you after a purchase

Keep an eye on your card during the transaction, and get it back as quickly as possible

Carry your cards separately from your wallet, in a zippered compartment, a business card holder, or another small pouch

Keep a record of your account numbers, their expiration dates, and the phone number and address of each company in a secure place

Best Practices: Ways to Protect Your Credit Cards (cont'd)

Never sign a blank receipt

Report lost or stolen cards immediately

Destroy unwanted cards to avoid misuse

Maintain a list of all your cards and their respective numbers, which is useful when lost or stolen cards are reported

Never give your card number over the phone unless you are dealing with a reputable company

Report any questionable charges promptly and in writing to the card issuer



Summary

E-Crime is a term used to classify investigation of criminal offences, where computers or other electronic devices have been used in some manner to ease the commission of an offence

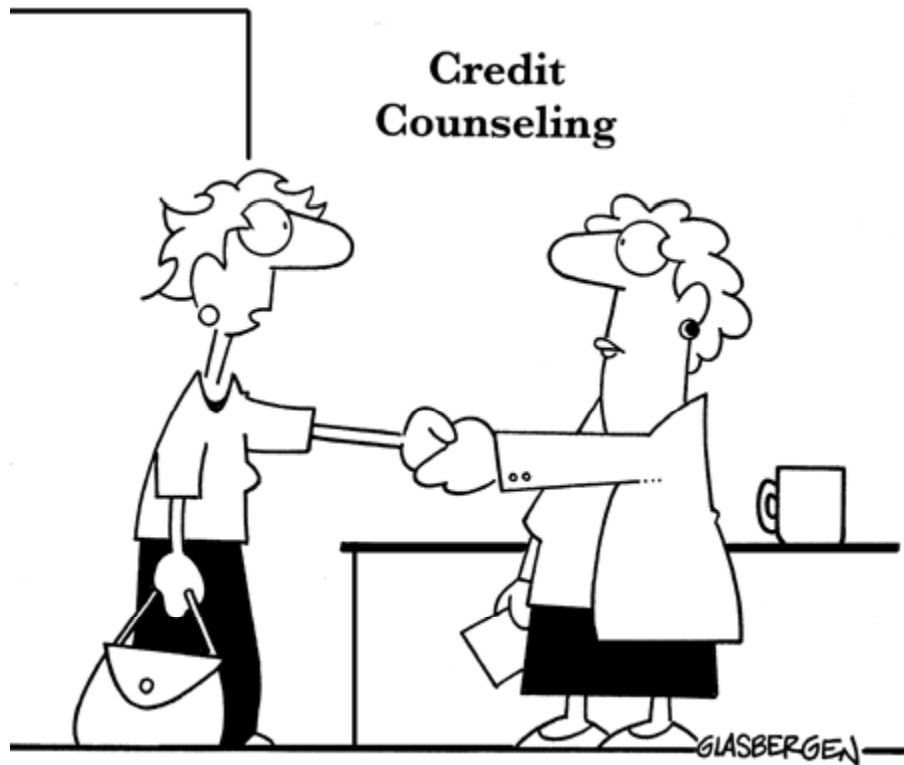
Theft and fraud carried out using a credit card or any alike payment mechanism as a fake source of funds in a transaction

When you use a credit card, you can be vulnerable to fraud, whether you pay online, over the phone, or even in person at your neighborhood grocery store

Credit Card Generator software that generates credit card details to fool the basic checks which certain online stores do when you pay for goods

© 2007 by Randy Glasbergen.
www.glasbergen.com

Credit Counseling



**“Sorry I’m late. I had to borrow against my 401k
to get money for the parking meter!”**

Copyright 2002 by Randy Glasbergen.
www.glasbergen.com



“Trickle down economics...that’s when you check your investments and something starts to trickle down your cheek.”