

# Chapter 1

## Intoduction

The advent of credit cards and their increasing functionality have not only given people more personal comfort, but have also attracted malicious characters interested in the handsome rewards to be earned. Credit cards are nice target for fraud, since in a very short time a lot of money can be earned without taking many risks. This is because often the crime is only discovered a few weeks after the date. Credit card fraud can be defined as unauthorized account activity by a person for which the account was not intended. Operationally, this is an event for which action can be taken to stop the abuse in progress and incorporate risk management practices to protect against similar actions in the future. In simple terms, credit card fraud is defined when an individual uses another individuals credit card for personal benefit while the owner of the card and the card issuer are not aware of the fact that the card is being misused. And the person using the card has not at all having the connection with the card holder or the issuer and has no intention of making the repayments for the purchase they done.

## Chapter 2

# DIFFERENT TYPES OF FRAUD TECHNIQUES

There are three classes of frauds namely card related, merchant related and internet frauds. Some of them are listed below

### 2.1 Card Related Frauds

#### 2.1.1 Lost/Stolen Card:

This type of fraud occurs when the fraudster simply steals a customers card. In this case, the customer might feel he has lost his card, but actually this card might have been acquired by an attacker.

#### 2.1.2 Account Takeover:

This type of fraud occurs when the valid customers personal information is taken by fraudsters. The fraudsters takes control of a legitimate account by either providing the customers account number or the card number. The fraudster then contacts the card issuer, as the genuine card holder, to ask the mail to redirect to a new address. The fraudster reports card lost and asks for a replacement to be sent.

#### 2.1.3 Cardholder-Not-Present (CNP):

CNP transactions are performed only on the internet that is remotely, in such kind of frauds neither the card nor the cardholder is present at the point-of-

sale. This takes many types of transactions such as orders made over the phone or Internet, by mail order or fax. In such transactions, retailers are unable to physically check user or identity of the card holder which makes the user unknown and able to disguise their true identity. The details of the credit card are normally copied without the cardholders knowledge, collected from the receipts thrown by the customer or obtained by skimming process. Frequently obtained card details are generally used with fabricated personal details to make fraudulent CNP purchases. This means that while the three or four digit card security code (CVV number) on the back of cards can help prevent fraud where card details have been obtained, but when the card is stolen it won't be helpful.

#### **2.1.4 Fake and Counterfeit Cards:**

This is another type of fraud where the creation of the counterfeit cards, together with lost or stolen cards poses highest threat in credit card frauds. Fraudsters are constantly finding new and more innovative ways to create counterfeit cards. The below mentioned are some of the techniques used for creating false and counterfeit cards.

#### **2.1.5 Erasing the Magnetic strip:**

This is the type of fraud where the fraudsters erase the magnetic stripe by using the powerful electromagnet. The fraudsters then tamper with the details on the card so that they match the details of a valid card, which they may have attained, for example, when the fraudster begins to use the card, the cashier will swipe the card through the terminal several times, before realizing that the metallic strip does not work. The cashier will then proceed to manually input the card details into the terminal. This kind of fraud is having high risk because the cashier will be looking at the card closely to read the numbers.

#### **2.1.6 Phishing:**

Phishing is a type of fraud designed to steal a person's identity. It is usually committed via spam e-mail or pop-up windows. Phishing works by a malicious person sending lots of false emails. The emails look like they have come from a website or company you trust, for example your bank. The message tells you to provide the company with your personal details including your payment card details. They can claim that the reason for this is a database crash or something like this. To make the email look even more authentic, the fraudster might put a link to a website that looks exactly like the real one but in fact that is not the real one and that is the fake one. These copies are often called Spoofed websites. When you are on the spoofed site they can ask you for even more personal details that will be directly transmitted to the person who made that website.

## **2.2 Merchant Related Frauds**

### **2.2.1 Merchant Collusion:**

This type is done when a merchant purposely passes on his customers personal information to fraudsters.

### **2.2.2 Triangulation:**

Here, the fraudster creates a fake website and operates from there. Many discounts are given to the customers through this website due to which users are attracted to such websites. They purchase items and there they enter their personal information. Then this information is obtained by the fraudsters and they use it to perform illegitimate transactions.

## **2.3 Internet Frauds**

### **2.3.1 False Merchant Sites:**

In this type, the website asks the customers to enter their personal details if they want to access the content of the website. In this way, these fraudsters collect many credit card number which they use later for performing fraudulent transactions.

### **2.3.2 Keystroke Loggers:**

Keystroke logger is a spyware which infects a users computer unknown to him. This spyware tracks all the details typed by the user and gives this information to the fraudster who thus obtains all the personal details.

### **2.3.3 Cell phone camera Scan:**

When a customer is paying his bills, a fraudster may be roaming somewhere near him. The customer may be under the assumption that the attacker is busy chatting on his phone, but actually he is taking digital image of the computers details such as card number, expiry date, etc. This type of fraud is possible because of powerful cameras used these days.

### **2.3.4 Site Cloning:**

Site cloning is where fraudsters clone an entire site or just the pages from which the customer made a purchase. Customers have no reason to believe they are not dealing with the company that they wished to purchase goods or services from because the pages that they are viewing are identical to those of the real site. The cloned site will receive these details and send the customer a receipt of the transaction through the email just as the real company would do. The customer suspects nothing, while the fraudsters have all the details they need to commit credit card fraud.

## Chapter 3

# PROBLEMS WITH CREDIT CARD FRAUD DETECTION

One of the biggest problems associated with fraud detection is the lack of both literature providing experimental results and of real world data for academic researchers to perform experiments on. This is because fraud detection is often associated with sensitive financial data that is kept confidential for reasons of customer privacy.

We now enumerate some of the properties a fraud detection system should have in order to perform good results.

- The system should be able to handle skewed distributions, since only a very small percentage of all credit card transactions is fraudulent, To solve this problem, often the training sets are divided into pieces where the distribution is less skewed.
- The ability to handle noise. This is simply the presence of errors in the data, for instance incorrect dates. Noise in actual data limits the accuracy of generalization that can be achieved, no matter how extensive the training set is. One way to deal with this problem is by cleaning the data.
- Overlapping data is another problem in this field. Many transactions may resemble fraudulent transactions, when actually they are legitimate. The opposite also happens, when a fraudulent transaction appears to be normal.
- The system should be able to adapt themselves to new kinds of fraud. Since after a while successful fraud techniques decrease in efficiency, due to the fact that they become well known. Then a Good fraud tries to find new and inventive ways of doing his job.

- There is a need for good metrics to evaluate the classifier system. As an example, the overall accuracy is not suited for evaluation on a skewed distribution, since even with a very high accuracy, almost all fraudulent transactions can be misclassified.
- The system should take into account the cost of the fraudulent behaviour detected and the cost associated with stopping it. For example, no profit is made by stopping a fraudulent transaction of only a few Euros.

This means that there should be a decision layer on top of the fraud detection system. The decision layer decides what action to take when fraudulent behaviour is detected via the fraud detection system, taking into account factors like the amount of the transaction and the quality of the customer doing the transaction

## Chapter 4

# ARTIFICIAL NEURAL NETWORKS

### 4.1 Definition

Neural Network exists in many ways and different forms. The type of neural network we will discuss in this paper is the Feed Forward Multilayer Perceptron. A feedforward multilayer perceptron consists of different layers of perceptrons that are interconnected by a set of weighted connections. We can distinguish three types of layers:

#### 4.1.1 Input

Input layer Receives input from an input stream, which can be database or some device or something else.

#### 4.1.2 Hidden Layer

Is hidden from the outside world and receives input only from the input layer or another hidden layer

#### 4.1.3 Output Layer

Connects the network to the outside world again and provides the final output of the network

A feed forward multilayer perceptron has no cycles and there is full connectivity between the perceptions of two consecutive layers. Signals can be propagated in two directions: function signals are propagated forwards, i.e. from input layer through the hidden layer(s) to the output layer and error signals are propagated backwards, i.e. from output layer through the hidden layer(s) to the input layer.



## 4.2 Learning

The type of learning we will discuss is commonly called supervised learning or error correction learning. The algorithm that we have used to do this is called Back Propagation of Error signals or in short Backprop. Every iteration of the algorithm consists of two passes:

### 4.2.1 Forward Pass:

Forward pass every perceptron calculates the weighted linear combination of all its inputs and applies to the result of this summing junction an activation function. The result of the activation function provides the perceptron of its output value.

### 4.2.2 Backward Pass:

At the output layer of the network we calculate the error with respect to the desired output value for a certain pattern. This error is propagated backwards through the network enforcing a correction on the weights of all connections in the network. This technique is based on the observation that all perceptrons in the network have a shared responsibility for the error that has been calculated at the output layer.