ROOT CAUSE ANALYSIS OF CREDIT CARD FRAUD DETECTION

Abstract.

Fraud is a widespread problem in the financial industry with devastating effects. It is essential to prevent and reduce fraud effectively. Traditional approaches, such as expert system, suffers from the incapability to handle complex problems and tremendous amount of data, while the recent development of various machine learning techniques brings new solutions. With many research works focusing on tackle frauds of credit card transaction or insurance, only few mentioned the identity fraud of credit card application.

Introduction.

Financial fraud is a criminal act, where fraudsters profit illegally by deceiving or stealing personal information. Fraud may affect the development of industry, undermine economic stability, and reduce people's wealth. For a long time, it has been a huge concern for banks, companies, and individuals. About 10% of insurance pay-outs are caused by fraudulent claims. According the Federal Trade Commission of the USA, in 2019 alone, 1.7 million frauds were reported with a staggering loss of $1.9 billion. Over the years, with the change of fraud detection methods, the fraudulent party has also continuously changed the fraud methods in order to avoid the tracing. With the development of the CISAI 2020 Journal of Physics: Conference Series 1693 (2020) 012064 IOP Publishing doi:10.1088/1742-6596/1693/1/012064 2 internet and online services, the number of frauds has recently increased. Credit card fraud and identity theft account for 20% of the total fraud and is becoming a big issue. Fraudsters use wrongly or illegally obtained identities to conduct credit card transactions or apply for new cards to avoid paying bills. Therefore, a reliable method of analysing and detecting fraud is essential to the safety and prosperity of online financial activities. The traditional approach to identify frauds is expert system, which is a set of rules made by experts, and will determine whether a transaction is fraudulent or not. However, as financial systems get more and more complicated, the number and complexity of rules grow to a point where no one could construct and maintain such complex system. As a result, more and more attention has been focused on machine learning and data mining. Instead of writing rules by hand, computers can learn the patterns and signals of fraudulent activities and identify potential frauds based on some relatively simple algorithms. And with the development of more powerful and tailor-made hardware for training such models, handling huge data sets containing billions of records became plausible. Researchers have been building such models with a wide range of algorithms and achieved excellent accuracy. Most research, though, focused on credit card payment or transactions, but the area of identity theft, especially for credit card application, remains open variables.

How it happens and why it happens:

In today’s world the usage of credit card become normal even in developing countries also. For every smallest payment user depends on credit and debit card such as shopping, important bill payments and money transfer. Most of the card holders have multiple credit cards. The financial frauds are one of the most common frauds in private as well as in the government sectors. Credit card fraud can be internal and external fraud the purpose of both type of frauds is to financial status of individual.

Internet service, mobile phone, e-banking and other devices responsible for credit card fraud. These types of criminal activities are committed due to the inattentive behaviour of the user. Phishing, Vishing, Mishing and Smishing are most common cyber-attacks that can collect information's of the cards detail for performing fraud. Sometimes the end users are not aware about that some kind of cheating in done with their account. For detecting and identifying attack the organizations and banking companies follows the different data mining, machine learning technologies and artificial intelligence tools [5]. Other mathematical algorithms and pattern-based models are implemented. These pattern-based models checks that the incoming transactions are original or not. The credit card frauds are based on some parameters such as sensitivity, accuracy, efficient, precision, specificity and so on. Data mining and machine learning technology develop tools for detect the rate of fraud with financial term.

How to protect yourself from credit card fraud:

Keeping the Credit Card Safe:

The primary step for credit card fraud prevention is to keep the credit cards in a place which is not easily accessible for others. First, make sure that a new credit card kit/envelope is not tampered with, and sign on the back of the card as soon as you receive it. Always keep the credit card secured in a small wallet which will make it difficult for snatchers or pickpockets. After every purchase, one must never forget to put the card away as soon as possible because thieves can store a digital imprint of the credit card through snapshots using cell phone cameras. It is also recommended to confirm the possession of the credit card in your wallet from time to time, even if you have not used it in a while.

Monitor Credit card transactions online:

Banks allows you to monitor your credit card transactions via SMS and email alerts and also via Online Banking or SC Mobile. You can get real time alerts that enables tracking of credit card spends.

Avoid Paper Trails of your Credit Card Number:

This is another simple step for avoiding credit card fraud. Credit card billing statements usually have the full credit card number printed on them. As a credit card user, one must always remember to shred the statement before dumping it into the bin. Expired and cancelled credit cards should also be shredded.

Signing of Blank Receipts:

The amount on the credit card receipt should be thoroughly verified before signing the bill. In case of a credit card receipt with blank spaces, it is advisable to fill the blank spaces with zero/s (0) or scratch through before putting the signature.

Never Make Credit Card Information Public:

Always be aware of scammers and potential threats of phishing. Credit card number and other sensitive information related to the credit card should never be provided over the phone or through text messages. Credit card scammers usually pose as new service issuers or providers of lucrative business offers while tricking the unsuspecting user into leaking sensitive information about the credit card. Ensure that you memorise your PIN and change it frequently to avoid misuse. You can change the PIN for your Bank credit cards online, by following simple steps here.

Double-Check Your Online Transactions:

Credit card providers be aware of the phishing threats posed through email links that mimic bank logos, credit card provider or businesses that require personal information. A general rule of thumb is to verify the legitimacy of the online website that you are making the purchase from. This can be done by checking if another website of the same or similar name exists. Always make sure that the website is secure by checking for the 'https://' in the address bar of the site. Exercising caution goes a long way to avoid credit card fraud.

Immediate Reporting of Lost or Stolen Card:

It is advisable to report a lost or stolen card to the service provider as soon as possible. As a customer, you must remember, the sooner the intimation of a lost card, the quicker the credit card fraud prevention. Always keep the credit card company's customer service number in your phonebook to avoid delays in informing the service provider in case of credit card loss or theft. Only with prompt reporting can one avoid credit card fraud in such cases.

Review the Billing Statement:

Another necessary step for credit card fraud prevention is consistent review of the billing statement for each month. Unauthorized charges are a sure sign of credit card fraud. Under such circumstances, the extent of the fraud is immaterial, as even a small unauthorized charge should be reported immediately to the credit card service provider. Usually, in this case, the service provider will instruct you to close the account and apply for a new account number. At Standard Chartered, the user gets an SMS and email notification each time the credit card is used. In case of unauthorized transactions, it is recommended that you report it immediately and block the card.

Making Strong Passwords:

In this digital age, credit card numbers are usually stored online for the ease of access and one-click purchases. A basic rule for making a strong password at some of the most secure websites is to use a combination of both upper- and lower-case characters and numbers. It is also advisable to memorise the password and avoid jotting it down on a piece of paper for future reference.