RESEARCH INSIGHTS

D Vinoshini
dv001@mymail.sim.edu.sg

Financial Fraud Detection: *A Framework*

Financial crimes are a prevalent threat in today's global economic climate. As a financial hub, Singapore is certainly not immune to this. Let's delve into what goes on behind the process of keeping our finance system clean.

Overview

There is a wide array of financial crimes such as insider trading and market abuse, fraud and offences, bribery and corruption, money laundering and terrorist financing. In this essay our main point of focus will be money laundering and financing terrorism.

Fraud prevention describes the security procedures in place to prevent unauthorized users from initiating transactions on accounts they are not allowed access to. Despite the numerous advanced fraud prevention techniques available for online banking applications, it is possible for them to fail. *Fraud detection* consists of identifying such unauthorized activity once the fraud prevention has failed.

In recent years, advances in modern technology such as the internet has resulted in an increase in financial fraud. Higher credit card distribution has resulted in increased expenditure, but it has also led to an increase in fraud. Fraudsters are continuously improving their techniques, thus detection methods must be able to keep up.

In practice, fraud detection must be used continuously, since the system is unaware that fraud prevention has failed. Phishing is one of the most popular methods used by fraudsters to gain account information for authentication purposes from customers. Phishing's most prevalent technique is social engineering. Social engineering usually comes in the form of e-mails or text messages trying to convince users to open attachments or by directing them to some fraudulent site, and most of the time it is so well designed that many customers are led to informing their account details. A recent example would be the OCBC customers, who were misled into divulging their bank details to scammers. There were at least 469 victims that were affected by an SMS phishing scam, the losses incurred by the victims amounted to $8.5 million.

Overview of Singapore's Anti-Money Laundering / Counter-Financing of Terrorism (AML/CFT) framework.

Measures put in place:

- Robust AML/CFT legislation
- Close partnership with the business community
- Strict enforcement action and ongoing supervision
- Active international cooperation

There are 6 strategies implemented by the Financial Investigation Division of CAD (Commercial Affairs Department) to focus on money laundering investigations in Singapore, regardless of whether the money laundering offence arose from a domestic or foreign predicate offence and deprive criminals of the proceeds and instrumentalities of their crimes (both domestic and foreign), or of property of an equivalent value. The following strategies are:

Strategy 1: Ensure that money laundering is pursued in all appropriate cases, including those arising from foreign predicate offences.

Strategy 2: Promote effective international cooperation

Strategy 3: Asset Confiscation as a Desired Outcome

Strategy 4: Address money laundering risks identified in National Risk Assessment (NRA)

Strategy 5: Strengthen collaboration with Suspicious Transaction Reporting Office (STRO)

Strategy 6: Attention to emerging trends/Reduce "unknown unknowns"

History – before technology, how was fraudulent activity detected?

Early fraud detection studies focused on Statistical models such as logistic regression and neural networks. In 1995, Sohl et al. first predicted financial statement fraud using a back-propagation neural network. In 2004, Zhang et al. employed various data mining approaches to financial fraud detection, in addition to investigating financial scenarios such as stock market and bankruptcy prediction. In 2005, Vatsa et al. studied a novel strategy using game theory, in which fraudsters and detection methods were modelled as rival participants in a game, each attempting to gain the biggest financial benefit.

Banks

In today's world, practically everyone has to deal with a bank, whether in person or online. Both the customers and the banks face the chances of been trapped by fraudsters. Examples of fraud include insurance fraud, credit card fraud, accounting fraud, etc. Detection of fraudulent activity is thus critical to control these costs. Bank fraud detection can be done via the use of analytical approach, data-mining techniques, association, clustering, forecasting, classification, and the use of Artificial intelligence (AI), to analyse the customer data in order to identify the patterns that can lead to frauds. Upon identification of the patterns, adding a higher level of verification/authentication to banking processes can be added.

Let's look into how artificial intelligence is utilised by Bank fraud experts in more detail. They use technology to track scammers' movements and predict what they'll do next. Banks and the police have devised systems that monitor transactions on an unprecedented scale using machine learning and data analytics. The Anti-Scam Centre (ASC) of the Singapore Police Force has announced that robotic process automation has been integrated into its operations. It establishes a uniform method for communicating information on questionable accounts with banks, allowing them to anticipate fraudsters' next moves.

OCBC launched its fraud surveillance system in 2016. The bank's system can correctly identify transactions that are related to frauds. They rate the likelihood of the next transaction being fraudulent using a machine-learning algorithm. An alarm will be issued if the system identifies new behaviour on a new device, which they can use to identify money mules. They can then act on these accounts before the cash is transferred out. The system keeps track of online transactions and assigns a risk rating to each one. High-risk ones generate an alarm, which is subsequently investigated by a fraud analyst. According to OCBC's vice-president of fraud risk management, a machine-learning algorithm has increased the likelihood of successfully detecting fraud instances. The technology also records a user's regular finger motions and clicks on a device, as well as behavioural biometrics. The system would be able to track how a user navigates, backspaces, and uses autofill components, as well as their mouse movements and typing speed. Account takeover scenarios can then be identified, and fraud analysts can assess if an account is being utilized by a money mule. As fresh data points are uploaded, the algorithm continues to learn.

DBS Bank has its own fraud detection system that employs machine learning and artificial intelligence. They employ machine learning and artificial intelligence to discover transaction patterns of account usage, and then use all of the data points to determine whether this is a real customer or a potential scammer. This network connectivity analysis resembles a spiderweb. When an account is hacked, the type of transactions that occur through that account are examined. The information is then processed and displayed in a visual fashion, which helps link other fraudulent accounts and provides a comprehensive picture of entire scam operations.

Besides OCBC and DBS, UOB employs machine learning to help identify transactions that may be fraudulent. According to Mr Soh, head of investigations at the bank's Integrated Fraud Management department, "A combined approach with the whole banking community is needed so that we can all harness and build on technology together to complement our efforts to stop crime."

Case study: UOB's anti-fraud team thwarts scam and recovers funds in 30 mins

An elderly man's entire life savings was nearly swindled in a high-tech scam that took place in 2019. He normally only made transactions worth a few hundred dollars at most, when out of the blue there was a transaction of around $60,000. Despite never having performed a single foreign transaction, the system discovered that about 95% of the funds in this man's account were instantly transferred to an overseas account. After receiving an alert, UOB's Integrated Fraud Management Unit called the police and the customer, who verified he had not authorized the transaction. The team was quick in preventing the payment from going through. The bank's technology monitors all transactions in real time and employs machine learning and artificial intelligence with the help of which it took roughly 30 minutes or less to retrieve the funds from the time they received the alert

Systems in place

There are two complementary approaches for fraud detection, differential and global analysis.

The account usage patterns are observed and compared with the account usage history, which represents the user's regular behaviour, in the differential analysis approach. Any large divergence from the norm suggests the possibility of fraud.

In the global analysis approach, based on worldwide data, each device is watched and rated as real or fraudulent with a given probability. This is based on three assumptions. First, it is assumed that each device used for online banking has a single identification. The second assumption is based on the fact that the probability of a transaction being a fraud increases with the number of accounts accessed by the same source that requested the current transaction. The third assumption comes from the fact that the only way to know that a fraud has been perpetrated is when the customer reports it.

An empirical analysis performed on real-world transactions datasets revealed that most of online banking frauds had the following behaviour characteristics:

- Large number of different accounts accessed by a single fraudster.
- Transactions involving small values in many accounts.
- More payment transactions than usual in a single account.
- Increased number of password failures before the occurrence of frauds.

Data mining. The descriptive model points out the patterns or relationship in data and goes ahead to explore the properties of the data examined.

The use of result from data mining goes a long way to determine the data mining task to be performed. Data mining tasks are categorized as follows:

1. Exploratory Data Analysis: It is as simple as the name implies. Data is explored without any clear idea of what is being looked for.

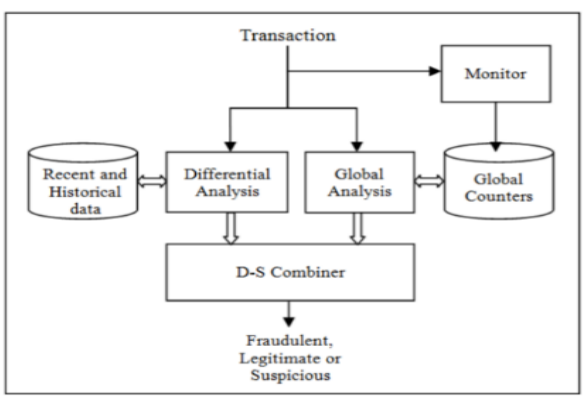
2. Descriptive Modelling: It describes all the data involved and models the relationship between every single variable.

3. Predictive Modelling: This model permits the value of one variable to be predicted from the known value of other variables.

4. Discovering Patterns and Rules: This is concerned with the detection of patterns and unravelling of fraudulent behaviour by exposing regions where data points significantly different from the rest.

5. Retrieval by Content: Here, patterns which are similar to the pattern of interest in the data set are figured out. It is mostly applicable to text and image data sets.

The figure below shows a general layout of the fraud detection system.



Source: ResearchGate, Online Banking Fraud Detection Based on Local and Global Behavior

In 2021, United nations estimated some $1.6tn is laundered every year, and authorities say lockdown measures have presented criminals with even greater opportunities to commit offences

Writer's Opinions

Financial fraud has far-reaching implications for the finance industry, government, corporate sectors, and consumers. In recent years, the problem has been exacerbated by an increasing reliance on new technologies such as cloud and mobile computing. Traditional techniques of detection rely heavily on auditing, in which a trained individual manually examines reports or transactions in an attempt to spot fraudulent activity. This strategy is not only time-consuming, costly, and erroneous, but it is also impractical in the age of big data. Furthermore, advancements in technology have rendered the traditional methods inefficient and unreliable due to the complexities associated with the problem. Financial firms, predictably, have turned to automated operations based on statistical and computational methodologies.

It can be challenging for banks to protect the online/internet banking channel. The challenge is in keeping customer's account secure while avoiding complexity in the login process. The myriad of passwords, hardware token devices and other out-of-bound communication tools introduced by some banks can be greatly discouraging to some customers. Online Banking Authentication is getting more complex as new threats are discovered and the technology needs to secure users against them. Authentication used to be a simple password but because of growing threats over the years it has grown from that to password with numbers, then to password with numbers, symbols, and special character, to knowledge-based questions and finally to the current state of external devices (token) and communication channels to verify transactions.

Despite all the measures in place, its not possible to omit the chances of fraudulent transactions taking place. However, it is safe to assume our funds in the commercial banks are almost are most likely secure thanks to quick thinking professionals and the advance systems put in place to deter fraud.