Jeffrey Semon

University of Maryland University College

1202 MSAS 670 9040

The Impact of Information Technology on the Role of Fraud

Information technology has found it's way into all aspects of our lives. We can see it in our personnel lives and we can see it at work. Cell phones and PCs permeate our personal lives while large computer networks help us do business at work. With all of this information technology in our personal lives and business lives there are those who would target the information technology for illegal purposes. We all see how fraud impacts information technology in our personal and business lives. The question is does all of this information technology that permeates our lives have a positive or negative impact on fraud.

There is a plethora of information to support the benefits that technology provides when it comes to fraud. In the following discussion there will be information presented that details how this is possible. One area that we can analyze is the Nigerian banking system and the benefits that information technology have provided in thwarting fraud. With regard to the Nigerian banking systems loans are a particular problem and the role that information technology plays in this area is significant. To elaborate, there is a large problem due to the lack of information technology that can be used effectively to curtail fraud involving loans. In Nigeria there is a lack of a standard national identification system, which would help establish an identity to anyone receiving a loan. We can observe how important of a control this can be when we imagine how easy it would be to steal an identity and obtain a loan with that information. There is also a lack of a central database that will promote information sharing about clients past indebtedness. This bit of information technology goes a long way at identifying high risk client's when it comes to making a decision about credit worthiness. This is important because it can help identify individuals who have constantly defaulted on loans. This lack of appropriate technology presents a problem in the Nigerian system because individuals

are now presented with the opportunity to intentionally take out loans with the intention of never paying them back. We can see how information technology makes a difference in combating fraud. In Nigeria there is also a problem with the system not being able to identify fake collateral that can be used for multiple loans. Once again, the absence of information technology makes itself apparent.

There are some solutions that information technology offers to remedy the problems that exist. One solution is the use of a biometric identity card. According to Ajah and Inyiama this will solve the problem of people creating multiple identities and perpetrating fraud with ease. Along with a national identity card there should be a central database to store the identities and personnel history. This will eliminate the use of the same collateral at different banks when perpetrators had a bad loan at another bank (2011, pp.5).

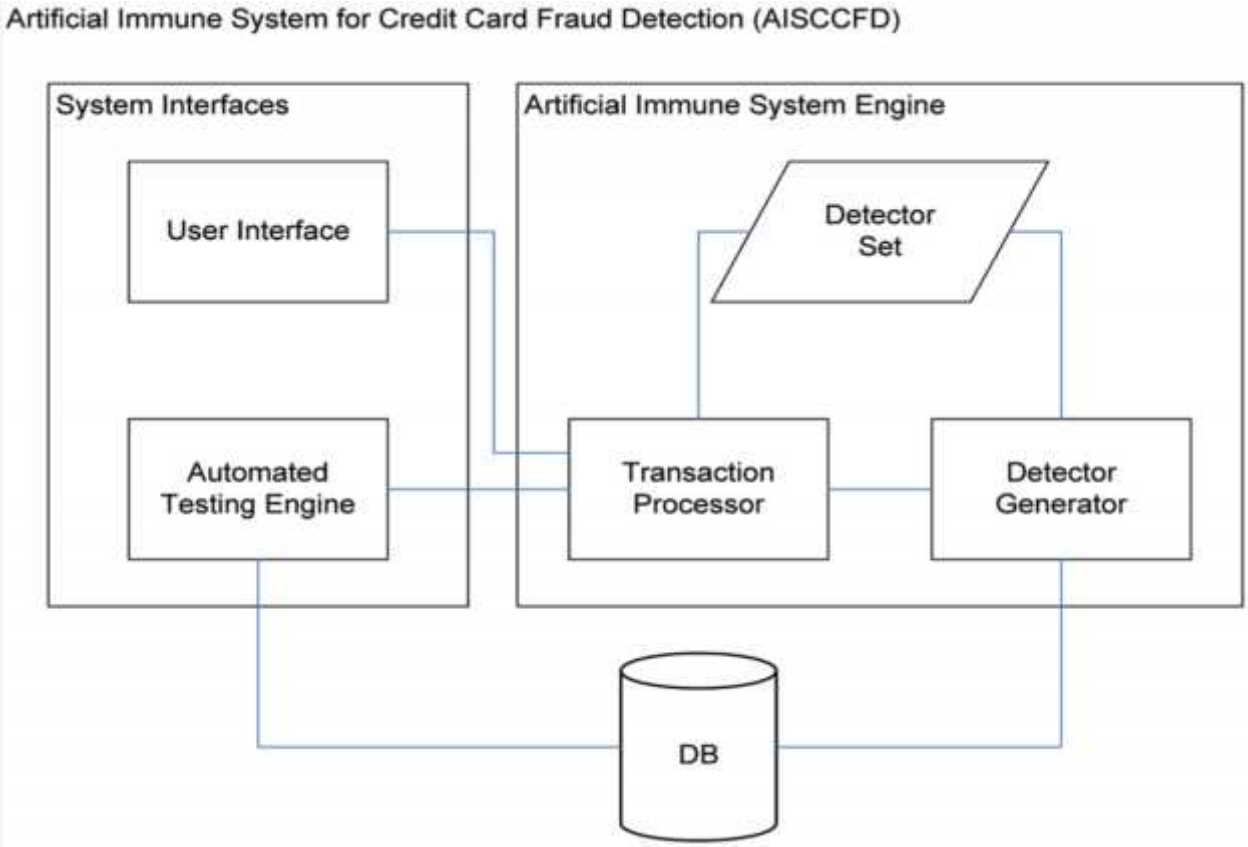
Artificial Neural Networks (ANNs) provide the analytical computing power to discover credit card fraud. Intelligent agents also have a place in the fight for fraud. Agents can be used to systematically monitor financial transactions. This can help detect high risk transactions, fraud and errors in financial transactions. Data mining can summarize and view data from unique perspectives making it a strategic tool in fraud detection. This unique perspective can be used to determine if a customer will be likely to defraud a bank and becomes useful when selling credit cards. A graphical information system (GIS) is an interesting system that can be used in concert with a global positioning system (GPS). In this system, properties locations can be integrated into the GIS to determine the validity of property when approving as a collateral in a loan.

Another area that is outside the area of loans that employs information technology on the cutting edge of today's fight against fraud is the area where fraud and mobile communications come together. In mobile communications there are large amounts of data. This data can be used in databases that can be used with rule based and neural network technologies that profile network subscribers and network traffic. The use of technology in this manner lends itself to one of the tactics in fraud examination, which is checking data for questionable signs in user behavior. According to Nonyelum, with this method, intentions of mobile phone users cannot be observed, but the intentions of the mobile phone user can be inferred from the mobile phone data (2010, pp. 34).

In the particular instance that we will be discussing next, information technology lends itself to a perpetration of fraud itself but the use of information from databases provides a possible solution to the problem. The problem that occurs is the cloning of cellular phones, which happens by using a mobile communications scanner to find the two identification numbers of the legitimate user's phone and copying them onto another phone. Information technology provides a possible solution by using databases to uses a phone toll ticket, which according to Nonyelum, is a bill issued by the network after each call, which contains all relevant information about the cell. The information contained in the toll is the International Mobile Subscriber Identity, the starting date of the call, the starting time of the call, the duration of the call, the number called, and the type of call (national or international) (2010, pp. 35). With the data in hand from the toll ticket filling up databases we can see how the data can be useful in determining if a fraud is occurring. Patterns can be used to build behavior profiles that are utilized by rule-based and neural network systems together.

There are more instances in the banking industry that lend themselves to innovative information technology when it comes to fighting fraud. Grid computing is one area that can be used to help fight fraud by using Service Oriented Architecture (SOA) as the framework for the grid. The SOA provides a framework for intelligent agents to take on the role of body, brain, facilitator and abilities. Basically, the agents in the system are taught the modus operandi of a specific fraud. This fraud knowledge is then spread across the grid as queries are made in the system in order to indentify banking frauds that are occurring. A practical example given to us by Paletta and Herrero is that an individual walks into Bank C and uses a bogus check. The bank employee later realizes this and uploads the perpetrator's picture from surveillance into the system. The perpetrator then goes to Bank A to try the same fraud again. The system searches the grid by checking with Bank B to determine if there is a fraud that exists there. There is not, so it checks with Bank C on the grid where the fraud has been documented. The fraud is identified by Bank A at this point and the fraud is stopped from being committed again (2009, pp. 321 - 322) .

Going back to a discussion regarding banking, we will examine the topic of credit card frauds and Artificial Immune Systems (AIS) used for the prevention of credit card fraud. AIS is designed to emulate the human bodies defense from complex biological attacks. Although this analysis focuses on credit cards, AIS can be used in many applications of eBusiness. The system is composed of the following on the next page 's diagram as discussed by Wong, Ray, Stevens and Lewis:



(2012, pp. 62)

One can see the flow of information in this system from the diagram. The detectors are used much like immune cells in the body. The AIS binds to certain algorithms that may represent an anomalous transaction much like a immune system bonds to an foreign antigen that can cause illness. According to Wong, Ray, Stevens and Lewis, the database allows for storage of the known fraudulent data as well as legitimate data, so that the system can maintain it's state between executions (2012, pp. 62). This type of information technology is in it's infancy and is thought to offer an alternative from rule based and neural network hybrid technologies, manual verification, CVC2, address verification service, programs such as MasterCard Secure Code and Verified by Visa, rule based systems alone and neural network systems alone. According to Wong, Ray, Stevens and Lewis initial analysis of the test results show that a fully

augmented AIS system may be a viable solution, due to the fact that it has a detection rate of 71.3 percent (2012, pp. 69).

Information technology may give us avenues to fight fraud effectively but it is also a tool that provides various methods to perpetrate fraud. One fraudulent method of attack that exists because of information technology is phishing. Pundir, Pradeep, Gomanse and Virendra define phishing as a fraudster using various attack vectors such as email, phone calls or text messages to try to occur an individual to click a link that takes you to a fraudulent website, where you are asked to disclose confidential financial and personnel information, like passwords, credit card numbers and primary account numbers (2011, pp. 25). The type of attack vector mentioned previously is called a URL obfuscation attack vector. There are other methods as well such as a Man-In-The-Middle-Attack. In a Man-In-The-Middle-Attack, the fraudster sets himself/herself between the user's computer and the real website. This allows the fraudster to monitor communications, putting the fraudster in a position to intercept valuable communications and use them for illicit purposes. Spoofing is also another method which fraudsters use information technology to perpetrate fraud. Spoofing consists of a fraudster creating a website to mimic a legitimate website. An individual is directed to this website and asked to divulge personnel identifiable information (PII). According to Pundir, Pradeep, Gomanse and Virendra, PII consists of information such as full name, last name, national identification number, primary account number, IP address, credit card numbers, digital identity, etc. (2011, pp. 25). Vishing is a combination of voice and phishing that is much like social engineering. The fraudster uses VoIP technology and imitates a legitimate company to obtain PII. Skimming is a method that is very popular at restaurants or shopping outlets. It

involves an individual that is employed at the establishment using a card reader to obtain the card information (PII) to be later used for transactions. The use of any of the above mentioned frauds then can be used to involve a "money mule". According to Pundir, Pradeep, Gomanse and Virendra, a money mule is an unwitting participant in the frauds who is recruited by the fraudsters to launder money across the globe. This is done at this point because the fraudster can use the compromised account to transfer funds out of and needs individuals to do the dirty work. If you have been in an active job search and posted your resume online you may have been contacted by fraudsters offering fraudulent work at home jobs that required you to wire money overseas for a commission. This is a money mule position. Carding is a strategy that uses IT to validate whether or not a credit card will be useful for making transactions. The fraudster uses the credit card to make a small purchase that is unnoticeable to the card owner to determine if the credit card is active. If it is, the credit card will be used later on the internet later for illicit purposes.

An area where information technology has had a negative impact on fraud in Nigeria is identified by Ajah and Inyiama. The problem the latter have identified pertains to the Credit Risk Management System (CRMS) that was used by the Central Bank of Nigeria (CBN) in the 1980s and 1990s to identify rising non-performing credit portfolios in banks. The system did not provide substantial credit history on a borrower to adequately guide a lender to make an intelligent decision on whom to grant the loan for (2011, pp. 4). This presents a problem because it facilitates the creation of bad loans. With the creation of bad loans banks began to protect their customers from the CBN, which was fraudulent. This had a negative impact on credit market performance.

As we can see there are positive and negative impacts that information technology has on the role of fraud. With the facts that have been presented one can conclude that information technology has had a positive impact on the role of fraud. Due to this conclusion has been reached because of certain facts that stands out. The case presented about the Nigerian banking system highlights the fact that information technology is important in combating fraud by looking at how technology controls improve the banking system. Although fraud exists in a manner that takes advantages of various applications of information technology, practices draw level to correct these problems. This is evident in the application of AIS systems, which is an evolution of combating fraud from stand alone rule based detection systems, stand alone neural detection systems and hybrid systems that consist of rule based and neural systems of detection. It is also evident in the case of cellular phone cloning. In this case, databases are developed over time and analyzed to detect fraudulent behavior, such as cloned phones. It is possible for one to deduce that as fraud becomes intertwined with information technology, technology will draw level and free itself from the problems that fraud creates.

References

Ajah I., Inyiama C. (2011). Loan Fraud Detection and IT-Based Combat Strategies. *Journal of Internet Banking and Commerece,16,* 1-14. Retrieved from Computers and Applied Sciences.

Nonyelum o. (2010). Fraud Detection in Mobile Communications Using Rule-Based and Neural Network System. *IUP Journal of Science and Technology, 6,* 35-43. Retrieved from Computers and Applied Sciences Complete.

Paletta M., Herrero P. (2009). Towards Fraud Detection Support Using Grid Technology. *Multiagent and Grid Systems, 5,* 311-324. Retrieved from Computers and Applied Sciences.

Pundir, Pradeep, Gomanse and Virendra (2011). Attack Vectors Used in Fraudulence Connection During Online Transactions. *International Journal of Machine Intelligence, 3,* 25-30. Retrieved from Computers and Applied Sciences.

Wong N., Ray P., Stevens G., Lewis L. (2012). Artificial Immune Systems for the Detection of Credit Card Fraud: An Architecture Prototype and Preliminary Results. *Information Systems Journal, 22,* 53-76. Retrieved from Computers and Applied Sciences.