The rise of identity theft in the us

With the rising cases of fraud in the world today, forensic accountants and internal auditors are charged with more responsibility to apply their investigative and accounting skills in understanding such frauds. Understanding the recent trends, issues and schemes of different fraud cases are significant in examination, investigation and in proposing solutions to address such cases. According to the US Department of Justice, “ the recent trends in fraudulent activities are alarming and something needs to be done in order to change the patterns for the better of everyone” (Finklea 18).

In the current economy, the businessmen are willing to offer service and sell goods to strangers in exchange for a word of assurance to make the payment, on condition, that the word is accompanied by data of a credit or account history. Thence, identity theft involves acquiring data from the second party to counterfeit the transaction, and in the process, the thief acquires the goods on account of the buyer.

With advanced technology, anonymous data-based transactions have been made available characterized by payment of goods through the credit card system. However, the retail trade in recent years is centered and dependent on consumer data and internet commerce (e-commerce). As such, the trade has rapidly grown, and a wide range of sellers in the corporate world has begun to trade with instant credits based on consumer’s credit reports.

The changes in the modern-day trade have lowered costs for the merchants and consumer, but this has opened more channels and opportunities for fraud. It is worth mentioning that public awareness of identity theft to a

personal level and a public policy level as well, is now a crucial issue which has increased substantially. An article with a phrase, ‘ identity theft’ from the US Newspapers fills the internet ranging from the 1990s up to now.

Even though credit card issuers attempt to advertise their efforts to prevent identity theft, the users and still claim they becoming victims of identity theft. Mainly, much of this concern is focused on the people exposed to advanced technologies including large and developed network databases.

In 1998, a statute directed the Federal Trade Commission (FTC) to institute a principal repository for complaints related to identity theft. In this essence, the commission was able to assist the victims as well as conduct consumer education on identity theft (Finklea 29). Empirical and theoretical literature and studies on the prevention of identity theft in the United States are still in their infancy.

Identity theft is the fastest growing form of crime in the world and involves unauthorized use of another person’s data for economic benefit. Usually, personal details such as bank account, Social Security number, credit card number, telephone calling card number, and other valued identification data are used by an unauthorized person for individual gain. In the United States, many people have become victims in fraud schemes related to identity theft and have incurred losses in billions of dollars.

In 2012, survey data indicated that about 12. 6 million people in the US may have fallen victims of identity fraudsters. In a recent case at the Home Depot, it was reported that hackers made away with close to 56 million credit- and debit-card numbers. Later on, it was revealed that they also stole

at least 53 million emails belonging to customers (“ Tag: Identity Theft” 23). Although Home Depot initiated a free identity protection program for those who were affected by the incident, nothing could be done to restore their stolen email addresses.

The most notable trend in that particular case is the fact that the culprits did not actually ‘ hack’ into the system, but planted a malware onto the systems in different Home Depot stores. In response to the incident, Home Depot moved swiftly to scrub off the malware from all Home Depot systems. They have since then developed a free identity protection for those who were affected by the fraud (“ Tag: Identity Theft” 26).

Another type of identity theft that is exploding in the US is the credit card fraud. Latest figures in the US Department of Justice point to a worrying trend of a 50% increase in cases between 2005 and 2010. In a major credit card fraud case, a 40-year-old Miami man Miguel Gonzalez was in August 2014 charged in Newark federal court and pleaded guilty to the charges. Gonzalez was charged for using stolen credit card data in which he spent $23 million in a period of three years.

According to the prosecution, “ he spent on buying homes, expensive jewelry, cars and a speedboat” (“ Tag: Identity Theft” 32). This particular case was an eye opener as to the new ways that fraudsters use to carry out their criminal activities. According to the filings of the court, the accused got the stolen credit card information from a black market vendor who he communicated with over the internet. Credit card account information was gotten when various companies and retailers’ databases were hacked into.

Investigators said “ Gonzalez was a ‘ major trafficker’ in stolen credit cards because he had at least two e-mail accounts which he used to distribute the stolen credit and debit cards. He also used the same accounts to receive stolen and counterfeit credit cards” (“ Tag: Identity Theft” 36). In a case involving credit cards, the nation’s third-largest retailer Target in December 2013 announced that thieves obtained credit and debit card information of close to 40 million customers.

According to Target’s spokesman, “ they obtained such information along with the names of the victims” (“ US Government Tackles Identity Theft” 83). In January, new revelations emerged that the magnitude of the breach was much bigger than earlier reported. It emerged that other personal contact information for close to 70 million more shoppers had also been compromised. With Target’s security breach, the fraudsters did not just swipe payment card numbers for 40 million customers; they also stole addresses and emails, for up to 70 million Target shoppers.

Concerns were raised over the possibility of such personal data being used for identity theft. A Texas woman Lauren Campbell reported to a CBS station KHOU-TV that following the Target hack, her personal data was stolen and a thief applied for cards in her name, purchasing different stuff ranging from toys to diamond rings (“ US Government Tackles Identity Theft” 97). In attempts to develop safer credit cards, the President in 2013 issued Executive Order dubbed BuySecure Initiative as a critical step in ensuring Americans’ safety through secure payments to and from the federal government.

The initiative which applies the Chip and PIN technology apply to both new and existing credit cards issued to government workers and other debit cards issued for benefit programs. With this technology, payment cards will contain embedded microchips in place of magnetic strips (Zients 67). According to the Federal Trade Commission (FTC), " the number of identity theft cases has increased considerably in the past few years". Some of the issues that have been mentioned by relevant authorities as those that complicate the process of identifying, examining and addressing fraud cases include; the advancement in technology and increasing globalization.

Advancement in technology has enabled criminals to carry out their activities with ease without being detected" (" Tag: Identity Theft" 36). Law enforcement agencies have continued to face challenges relating to the identification and apprehension of the identity of the thieves. It is hard to establish whether the said criminals operate within or without the borders of the US. Recent trends also show that as much as some of the criminals operate as individuals, the majority of them operate as part of larger networks of criminals or organized crime.

In response to the rising cases of identity theft, there have been various attempts to curb and reduce such cases. As an administrative effort, a task force was established in 2006 and charged with the responsibility of coordinating federal agencies' efforts to curb identity theft. The President's Identity Theft Task Force in 2007 proposed a number of recommendations to aid in combating identity theft in the US including legislative propositions to fill the identity theft-related inadequacies in the federal criminal laws.

The Congress in further efforts also gave direction to FTC to issue an Identity Theft Red Flags Rule. “ The red flags require that financial institutions and creditors with specified account types create and institute written identity theft prevention programs” (“ Tag: Identity Theft” 47). In 2007, the task force came up with a strategic plan that addressed four major areas; protecting individuals’ data from criminals, making it hard for the fraudsters to use individual’s data, providing assistance to the affected in detecting and recovering from identity theft incidents, and preventing identity theft through the prosecution and punishment for those found guilty.

Other recent changes to help individual victims also include the move by the Congress in 2008 to pass the Identity Theft Enforcement and Restitution Act of 2008. The legislation allowed for restitution to victims of identity theft for the time spent recovering from the effects of an actual fraud incident or threat of fraud (Zients 74). The AICPA has also been up and about in efforts to ensure that consumers are protected from identity theft.

In 2013, the association made significant recommendations to help in combating tax identity theft. With regard to tax-related fraud, they proposed the implementation of new processes that allow the verification of taxpayer’s addresses before paying a refund. Another recommendation as proposed by the AICPA relates to expanding the use of IRS’s IP PIN program, which is accessible by taxpayers who have in the past become victims of tax-related identity theft. The IP PIN could also be used instead of a Social Security number when filing a tax return (“ US Government Tackles Identity Theft” 113).

Works Cited

- Finklea, Kristin M. *Identity Theft: Trends And Issues* . Congressional Research Service, 2014.
- “ Tag: Identity Theft”. *Federal Trade Commission* , 2018, https://www. ftc. gov/taxonomy/term/262/type/federal_register_notice. Accessed 13 Nov 2018.
- “ US Government Tackles Identity Theft”. Vol 2015, no. 5, 2015, p. 4. *Elsevier BV* , doi: 10. 1016/s1361-3723(07)70046-5. Accessed 9 Nov 2018.
- Zients, Jeffrey. *The President’s Buysecure Initiative: Protecting Americans from Credit Card Fraud and Identity Theft* . The White House: President Barack Obama, 2014. Accessed 11 Nov 2018.