Financial Crime in Correspondence with Cybercrime

Jagriti Khanna Ahooja*
Rishab Sharma**

Vivekananda Journal of Research
January - June 2023, Vol. 13, Issue 1, 10-19
ISSN 2319-8702(Print)
ISSN 2456-7574(Online)
Peer Reviewed Refereed Journal
©Vivekananda Institute of Professional Studies-TC
https://vips.edu/journal/

ABSTRACT

Today, in the era of emerging technologies and the continuous advancement of technology, it has become a child's play to use an electronic device for illicit activities or use them for illegal purposes. We live in the 21st century, also known as the internet era, where everything is accessible with one simple click, be it bank details or company information. Every company, organization, and government office use electronic devices, be it for communication, data handling, processing information, or making documents. Without electronic means and devices, the world would come to a standstill. Electronic devices have become an integral and the utmost important part of human life. However, the concern is not the emerging technologies or the technological upgradation, but the misuse and the harm it may cause to the common public. Technology has certainly made life easier and has decreased the difficulties of certain tasks drastically but it has also increased the possibilities of illegal activities. Financial frauds have become more common now because humans are finding ways to go around the system by using technology to aid them in the task. The proliferation of information technologies based on computers and communication devices, as well as process optimization and computerization in all spheres of life, have blurred national infrastructure and economic borders.

Keywords – ***Cybercrime, financial fraud, cyber threat, frauds.***

* Assistant Professor, G.D. Goenka University, Haryana. E-mail: jagriti.khanna75@gmail.com
** Research Scholar, G.D. Goenka University, Haryana. E-mail: rishabhnfs@gmail.com

INTRODUCTION

An intentional act of deception involving financial transactions for personal advantage can be widely referred to as financial fraud. Fraud is both a criminal and a civil law infraction. Numerous fraud instances include intricate financial transactions carried out by "white collar criminals" such as corporate professionals who have criminal intent and specialized competence. Few acts which can be considered as financial fraud are ATM pin theft, credit/ debit card fraud, internet banking fraud, payment QR code scams, etc. Today, every person carries a smartphone with them that has apps linked to their bank accounts or digital wallets. These apps can be accessed by a simple pin or OTP (One time password). A basic hacking of the device can lead the delinquent to have access to a person's personal details or bank accounts. Fraudsters have a variety of ways to get in touch with their potential victims, including face-to-face meetings, letters, phone calls, text messages, and/ or emails. Internet fraud is the fastest-growing type of fraud due to various factors such as how challenging it is to verify the identities and legitimacy of people and businesses, simple tactics used by scammers to divert users to fake websites in order to steal their personal financial information, conceal their true location because of the global reach of the web etc. Additionally, these developments have contributed to the growth of an integrated global information ecosystem, in which anybody may access any information from anywhere in the world, manage their assets remotely, do business with international counterparties without having to meet in person, etc. At the same time, the information age has turned into a haven for criminal activity and a tool for it. Criminals no longer need to personally interact with their potential victims and brainwash their "targets." They only require a computer and access to the information and communication network, where they can access databases, bank accounts, and management information systems using computer viruses and other illicit software. In 2004, the global cybersecurity market was worth $3.5 billion, and in 2017 it was worth more than $120 billion. Before the most recent market assessment by Cybersecurity Ventures, the cybersecurity market increased by about 35X over the preceding 13 years. Global spending on cybersecurity products and services for defending against cybercrime is projected to exceed $1 trillion cumulatively over the five-year period from 2017 to 2021[1]. RBI report showed that about 1.38 trillion dollars of frauds were reported in the year 2021 -22[2]. Although, there is a time lag between the occurrence of the fraud and its detection but still the amount seems far too much. The World Economic Forum noted that fraud and financial crime was a trillion-dollar industry, reporting that private companies spent approximately

1 https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

2 https://www.business-standard.com/article/finance/rbi-annual-report-fy22-saw-more-bank-frauds-but-value-decreased-by-half-122052700468_1.html

$8.2 billion on anti-money laundering (AML) controls alone in 2017[3].

EVOLUTION OF FRAUD AND FINANCIAL CRIME

The reality is that cybercrime is just an evolution of traditional crime and has a direct impact on economic growth, jobs, innovation, and investment. Companies need to understand that in today's world, cyber risk is a business risk[4]. Institutions consider frauds and financial crimes separate and, with the growing pace of technology these crimes have become more sophisticated and easier to attempt from afar and not restricted by the destination of the wrongdoer or the victim. Frauds are generally considered crimes consisting of forgery, credit card scams, fake mail, OTP scams, etc. Financial fraud is generally considered a crime on a broader scale like money laundering, tax evasion, organized money racketeering, etc.

Financial crimes and frauds are not something that started a few decades ago, but in fact, they started centuries ago. Some of the financial malpractices at that time were[5]-

- Dishonest measurements and weights to deceive and trick the customers
- Dishonest exchange of money between nations and clans (currency exchange scams)
- Exorbitant usury (interest rates and hidden charges)
- Illegal possession of someone's property.
- Money lenders charging wrong/ high charges from people.

These activities were done by different modes, methods, and means but the purpose always remained the same, malpractice, wrongful gain, illegal dealings, etc. Over the period of time, only mode/ means/ methods changed, they evolved with the rise of technology.

The first insurance scam, which we are aware of, occurred around 300 BC, when a man named Hegestratos, a Greek merchant, tried to sink his own ship to claim the insurance amount. The man planned to take out the goods from the ship before sailing and then claim the insurance and sell the goods in the market.

The first pump and dump investment fraud happened in the year 1792, done by William Duer. The first case of embezzlement was in the year 1473[6].

3 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

4 Id.

5 https://businessforensics.nl/financial-crime-history/

6 Id.

FINANCIAL CRIMES IN THE MODERN ERA

In modern-day lifestyles, electronic devices are not just wants but they have become a need. Every single activity of our daily lives is almost reliant on them. At any given moment there are multiple data points that are gathering information of a person. This could be when sometimes a person has searched for an item on the phone or interacted while the phone was on and the applications on the device start sending suggestions and advertisements relating to that item later. The device we use carries sensitive data like a person's bank details, personal details, identity proofs & licenses, etc.

Financial crimes in the age of information era have leveled up too as they are now carried forward in different forms and are even specialized and digitized.

Crimes that are executed in the present are life insurance frauds, illicit loan sharking, money laundering, identity theft, cargo fraud, embezzlement, crypto exchange frauds, cryptocurrencies pump and dump scams, illegal money transfer via crypto, NFT scams, and many more. With the emergence of technology, it has become more difficult to trace and track illicit activities.

TYPES OF CRIME COMMITTED

Hacking: As per IT Act, 2000 hacking is defined as "Whoever with the intent of cause or knowing that is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking[7]" "backdoor" program installed in the machine. Hacker/ cracker needs to access the devices and for that, they use password decrypting software, also known as brute force attack, which enters billions of passcodes to break the security[8]. In 2008, a group of Russian hackers used malware to invade the heartlands website which led to the leak of 130 million credit/ debit card numbers[9]. Hacking also includes spear phishing, phishing, bot networks, Trojan horse,

Phishing: "Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their usernames, password, or other personal information to access their accounts for some reason. Customers are directed

7 Section 66 : Information Technology Act, 2000.

8 An Overview Study on Cyber crimes in Internet : Journal of Information Engineering and Applications ISSN 2224-5782 (print) ISSN 2225-0506 (online) Vol 2, No.1, 2012.

9 https://www.upguard.com/blog/biggest-data-breaches-financial-services

to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account." [10] Phishing assaults in the banking sector surged by 22% in just the first half of 2021 compared to the same period in 2020. For the same time period, attacks on financial apps climbed by 38%[11].

Carbanak attack: These attacks began in 2013. In these attacks, the criminals target the employees of the bank, and send them an email with the carbanak backdoor as a file. as soon as the employee opens the attachment, the carbanak is activated. Once it has infected the device, attackers observe the person's behavior for the bank's cash transfer system. After this, they alter the amounts and inflate the accounts and steal the funds. The attackers program the ATMs to dispense cash to the members of the gang waiting at specific times. The banking system was hit quite heavily due to these attacks and lost almost 1 billion dollars[12].

Money Laundering: Section 3 of The Prevention of Money Laundering Act, 2002 defines it as "Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of the offense of money-laundering[13]". This is one of the biggest white-collar/ Organized crimes which is committed in the country. It is directly related to corruption and the black money surge in society. In the modern era, new means like crypto aid the criminals, Since no personal information can be associated with the public keys involved in a transaction, they offer better anonymity than traditional payment options. Criminals register online accounts with exchanges that deal in digital currencies and accept fiat money from conventional bank accounts. Then, they begin a "cleaning" process (mixing and layering), in which they transfer funds into the bitcoin network utilizing tumblers, mixers, and chain hopping (also called cross-currency). Less-regulated the exchange, more the money is moved from one cryptocurrency to another, leaving a trail of funds that is nearly hard to follow[14].

Dark web: Dark web is a subset of the deep web. The dark web is a part of the internet that can only be accessed via special software and browsers. It allows operators and

10 H. Thomas Milhorn, "Cyber Crime – How to Avoid BecoMing a Victim", Universal Publishers, 2007. ISBN: 1-58112-954-8.

11 https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services

12 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

13 Section 3 : Prevention of Money Laundering Act, 2002.

14 https://www.insightsonindia.com/security-issues/money-laundering/cryptocurrency-and-money-laundering/

users to surf through net anonymously. The dark web makes users untraceable. The deep web and dark web are used for positive actions like circumventing government censorship, contacting and collaborating with journalist anonymously, contacting federal agencies, etc. However, the dark web can also be used for unlawful activities like money laundering, purchasing illegal items, etc. The dark web is also used for many illegal things other than above mentioned. As of 2022 June, a price index[15] was published that showed the items a person can buy on the dark web and few of the items were –

- Credit card details, account balance up to 5000 $ - 120 $
- Stolen online banking details, a minimum of 2000 $ account – 65 $
- Clone American Express and MasterCard - 18 $ to 20 $
- 50 Hacked PayPal logins – 150 $
- Crypto.com verified login – 250 $

These are just the tip of the iceberg, from forged documents to viruses, malware, and DDoS attack, a person can buy anything on the dark web. Since crypto had entered the market, it has become easier to transfer funds anonymously and the dark web provides a one-stop mega mart to shop for tools and materials to commit cybercrimes. Research was conducted which showed pre and post Covid activity on the dark web and the numbers were staggering. Data breaches increased from 7.9 billion records to 36 billion records, hacked records from 15.1 billion to 37 billion, and publicly reported breach incidents from 1784 to 2953. These numbers are still nothing as compared to the financial loss incurred. As per the report the financial loss skyrocketed to an astonishing 4 trillion from merely 3.5 billion[16].

In 2020, Mcafee reported that cybercrime cost the global economy more than 1 trillion $[17]. The financial strain is put on the whole world and it has been increasing constantly. Criminals are getting more tools as technology is growing and the world governments are not able to keep up with them. Lawmakers are in a bind on how to regulate these technological advancements and minimize illegal activities.

The FBI issued a “Flash Alert” in July 2020 to American businesses engaged in the financial, healthcare, and chemical sectors doing business in China regarding the potential

15 https://www.privacyaffairs.com/dark-web-price-index-2022/

16 Razaque, A.; Valiyev, B.; Alotaibi, B.; Alotaibi, M.; Amanzholova, S.; Alotaibi, A. Influence of COVID-19 Epidemic on Dark Web Contents. Electronics 2021, 10, 2744.

17 https://www.business-standard.com/article/technology/mcafee-report-says-cybercrime-to-cost-world-economy-over-1-trillion

targets by Chinese government using the mandatory tax software[18]. Cybercriminals are naturally attracted to the financial sector. It is, after all, where the money is. There have been fewer dramatic successes, which is a tribute to the intense effort the sector has put into cybersecurity, both at individual, and institutional levels, and collectively. However, this comes at a cost, with spending of up to $3,000 per employee on cybersecurity. A survey conducted in 2018 by the FS-ISAC found that financial institutions spend (depending on their size) between 6% and 14% of IT budgets for defense. With enhanced use of cyberspace and an increase in the pace of digitalization, the number of cybercrimes is also increasing. As per reports from Scheduled Commercial Banks, phishing related frauds are collated under the category of 'Phishing/ Vishing/ Skimming' by the RBI and State/UT-wise detail of fraud incidents, the amount involved and extent of loss, reported in the category 'Phishing/ Vishing/ Skimming' during the period from 2019-20 to 2021-22 were 13,951 cases of fraud[19].

TACKLING THE PROBLEM

To tackle these problems, the first and foremost step is to spread awareness among the common people. Currently, a handful of people understand the threat of cyber attacks and cyber frauds. People are still unaware of the danger technology poses. A huge part of the problem can just be solved with this step. Small scams and frauds will exponentially drop in numbers. Also, the reports of RBI only contain frauds of Rs. 1 lakh and above so many smaller frauds are not highlighted in them. The Central Government has taken a number of measures to strengthen the mechanism to deal with cybercrime in a comprehensive and coordinated manner, including raising awareness of cybercrimes, issuing alerts and advisories, building the skills and capacity of law enforcement personnel, prosecutors, and judicial officers, improving cyber forensic facilities, etc. To offer a framework and eco-system for LEAs and to deal with cyber crimes in a thorough and coordinated manner, the government has established the "Indian Cyber Crime Coordination Centre" (I4C). The I4C has also established seven "Joint Cyber Coordination Teams" to address the issue of jurisdictional complexity based on hotspots/areas for cybercrime by enlisting all the States/UTs to give a strong coordination framework to the LEAs[20].

There is an active cybersecurity and e-surveillance organization in India, known as the National Cyber Coordination Centre (NCCC). Its functions include coordinating the intelligence-gathering efforts of other agencies and screening communication metadata.

18 https://www.ic3.gov/media/news/2020/200728.pdf

19 https://pib.gov.in/PressReleasePage.aspx?PRID=1845004

20 *Id.*

Some have expressed concern that the organization may restrict residents' civil and private liberties because India lacks clear privacy laws. In order to avoid online obscenity, the MeitY designated the Indian Computer Emergency Response Team ("CERT-In") on February 23, 2003, giving it the power to issue directives for website banning under the IT Act. In *Jyothikumar Chamakkala vs State Of Kerala*[21], CERT is defined as "an Agency designated under Sec. 70B of the Information Technology Act, 2000 as amended by Act 10 of 2009."

The Audit Committee of the Board (ACB) may continue to oversee all cases of fraud in general, but banks are required to establish a special committee for the sole monitoring and follow-up of cases of fraud involving amounts of 1 crore and above. Most retail cyber frauds and electronic banking scams are less than 1 crore in value, so they might not get the Special Committee of the Board's necessary attention. It is essential that the Special Committee of the Board be briefed separately on this in order to keep them informed of the proportions of the fraud and its modus operandi because these scams are multiple in number and have the potential to reach huge proportions[22]. Other means which are advised to organizations are Separate departments to manage fraud, fraud review councils, fraud prevention practices. The most effective way to prevent frauds is to have a solid internal control architecture. The business/operations/support groups and the fraud risk management department regularly assess different systems and controls to close any gaps and strengthen the internal control structure. The following are some fraud protection measures that all organizations are advised to use.

Currently, we require a unified model which has a fully integrated approach towards cybercrime. Completely integrated strategy and risk management across the entire organization are accomplished by integrating the activities for financial crimes, fraud, and cybersecurity into a single framework. The model shares insights and has a single perspective of the client. Risk convergence improves enterprise-wide threat transparency and more clearly identifies the most significant underlying concerns. The unified approach also captures the advantages of scale across crucial functions, improving the bank's capacity to draw in and keep top personnel. Currently, this model is the best and the most effective, but it requires a significant change and adaptation to the new framework, making it difficult for the banking operations less accustomed to regulators[23]. Since the crimes are already intricately intertwined, it is now essential to integrate fraud and cybersecurity activities. Integration's improved data and analytics capabilities are now crucial instruments for threat prevention, detection, and

21 W.P.(C).No.35069/19

22 https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf

23 https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/financial-crime-and-fraud-in-the-age-of-cybersecurity

mitigation.

In order to prevent financial criminals from siphoning off funds, the "Citizen Financial Cyber Fraud Reporting and Management System" module has been introduced. For assistance with filing online cyber complaints, use the toll-free Helpline number "1930"[24]. To stop these crimes from happening and to expedite investigations, the Central Government has taken steps to raise awareness about cybercrimes, issue alerts, and advisories, strengthen the capability of law enforcement professionals, prosecutors, and judges, and train them in these areas. The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) has been established to provide free tools for detecting and eradicating dangerous software. The government is periodically performing cyber security simulated drills and exercises to enable evaluation of the preparation and posture of enterprises in the public and critical sectors[25].

Almost all cybersecurity reports end with suggestions for how organizations can strengthen their online safety and put established best practices into action. Among these ideal practices are-[26]:

1. Consistent use of fundamental security precautions
2. More openness inside organizations
3. Coordinating and standardizing cybersecurity needs
4. Educating staff members about cybersecurity.
5. Developing prevention and response plans

CONCLUSION

Criminal transgressions in the field of cybercrime are aggravating at a staggering speed and financial crimes are rising with the advancement of technology and are breaking through traditional & jurisdictional boundaries. Currently, we are at the start of the information/ technological era and thus need to be more prepared and proactive in dealing with the situation, as it would lay a foundation for upcoming rules and regulations. Several international organizations are implementing new regulations to contain cybercrime but it would require more than that as this problem severs international borders and even with several treaties and conventions, they may not be able to be implemented as they were meant to be. Financial institutions are spending a lot of their capital on increasing security measures

24 https://pib.gov.in/PressReleasePage.aspx?PRID=1845004

25 https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579226

26 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

yet new ways and methods keep coming up. Also, the larger part of the problem remains is the percentage of the unaware population, as more people become aware the situation may tend to get better and the amount of financial fraud will start to decline. Moreover, the field of cyber security and data privacy is also expanding and is trying to tackle the problem at the grass root level which will benefit in the long run. Cyber is the most up-and-coming phenomena whether it be security, legal, financial, healthcare, educational, or even crimes. The faster we can grasp the change, the quicker we will be able to act on it as there is a causal nexus between the identification of problem and solving the problem.