International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Banking Fraud Identification and Prevention

R.A. Monalisha[1], Ms. T. Vaishali[2]

[1]B.Sc.(chemistry)., LLB(hons).,LLM(Pursuing)
School Of Excellence in Law, The Tamilnadu Dr. Ambedkar Law University,
Tharamani campus, Chennai
[2]B.A(Eng. Lit)., L.L.M.,NET., Ph.D.(Pursuing)
Assistant Professor Of Law
SOEL, The Tamilnadu Dr. Ambedkar Law University, Chennai

Abstract
The integration of information technologies in the banking sector and their widespread adoption in various financial activities have given rise to banking fraud and scams. As the foremost challenge in the banking sector, fraud and scams directly affect the well-being and prosperity of the global economy and individual nations. The magnitude of bank fraud cannot be known because much of it is undisclosed or undetected. To address this issue, our research focused on comprehending the technological dimensions and manifestations of bank fraud and scams, while also examining the response of governments and financial institutions in preventing and controlling such illicit activities. By surveying users of banking services, some of whom have fallen victim to fraud, and conducting interviews with experts from the financial industry, we successfully identified the most prevalent types of banking fraud and scams. We then compared the perspectives of these two groups to gain a comprehensive understanding. The findings of this study have significant implications for various stakeholders, including government agencies, citizens, corporate managers, financial and nonfinancial institutions, as well as academics seeking to enhance their knowledge about fraud detection and mitigation.

Keywords: financial services industry, banking fraud, scams, financial crime

INTRODUCTION

In recent years, significant strides have been made in the finance sector by incorporating information technology to achieve key business objectives. The reliance on modern information technology has become so crucial that it is inconceivable for any financial institution to function effectively without it, [1]. The primary purpose of technology in this context is to enhance the lives of citizens and streamline business transactions, simplifying processes[2]. However, the integration of information technologies in

[1]Stephen Mason, Nicholas Bohm, "Banking and Fraud," Computer Law and Security Review, The International Journal of Technology Law and, 2016.

[2] David Airehrour, Nisha Vasudevan Nair, Samaneh Madanian, "Social Engineering Attacks and Countermeasures in the New Zealand
Banking System: Advancing a User-Reflective Mitigation Model," Security in the Internet of Things, vol. 9(5), 2018.

banking and finance has also given rise to a novel form of criminal activity – banking fraud, wherein deceptive methods are employed to accomplish fraudulent goals and scams[3].

Despite substantial financial resources dedicated to combatting fraud and scams, it is surprising that the modern financial sector, according to The Association of Chartered Fraud Examiners (ACFE), is experiencing a growing vulnerability to fraudulent activities due to ineffective controls. This inability to safeguard not only the industry itself but also its customers is a concerning trend[4]. Moreover, the risk of financial crime is pervasive across all types of businesses, regardless of their development status, and its scale varies significantly[5]. As per the ACFE's estimations, the global cumulative annual loss resulting from bank fraud exceeds 3.5 trillion US dollars and continues to escalate annually.

Over a decade ago, banking fraud and scams rapidly spread and engulfed the banking sectors of numerous countries, including the United States of America (USA), Russia, Europe, and China. Recently, in 2020, these fraudulent activities also made their way to New Zealand[6]. The actual occurrences of such incidents are likely much greater than the reported figures, as many victims might not even be aware that they have fallen prey to fraud or may feel too embarrassed to report it[7].

Fraud within the banking sector poses a critical issue as it directly affects the global economy's well-being and the prosperity of individual countries[8]. The term "fraud" encompasses various meanings but is commonly used to refer to detrimental occurrences like civil or criminal offenses, misrepresenting the identity of individuals or organizations, and unfair transactions or contracts between parties resulting in harm to one of them[9].

According to [10], banking fraud refers to intentional illegal acts or omissions conducted during or in preparation for a banking transaction, to gain unlawful profits and cause financial harm to both the bank and its customers. Another, more contemporary definition of banking fraud, as proposed by the authors of, characterizes it as a deliberate act by an individual or a group to manipulate financial facts for personal monetary gain, using tricks (scams) and technological advancements (know-how). The authors in, strongly emphasize that fraud necessitates three essential elements: Will, Opportunity, and Exit (escape route), which they term "WOE."

[3] Umaru Hussaini, Arpah Abu Bakar, Muhammad-Bashir Owolabi Yusuf, "The effect of fraud risk management, risk culture and performance of banking sector: A conceptual framework," International Journal of Multidisciplinary Research and Development, vol. 6, no. 1, pp. 71-80, 2019.

[4] A.O. Enofe, T.O. Abilogun, A. J. Omoolorun, E. M. Elaiho, "Bank Fraud and Preventive Measures in Nigeria: An," International Journal of Academic Research in Business and Social Sciences, vol. 7(7), 2017.

[5] P. K. Ozili, "Advances and issues in fraud research: a commentary," Journal of Financial Crime, 2020

[6] S. Islam, "Enhanced Information System Security in Internet Banking and Manufacturing," International Journal of Engineering Materials and Manufacture, vol. 5(2), 2020.

[7] "Romance Scams," 13 02 2023. [Online]. Available: https://netsafe.org.nz/romance-scams/. [Accessed 14 03 2023].

[8] Ali Hakami, Tahani, Mohd Mohid Rahmat, "Fraud prevention strategies: the perception of Saudi Arabian banks employees," Asian Journal of Accounting and Governance, pp. 71-83, 2019.

[9] S. R. Tawiah, "Combating Fraud – The Role of Forensic Auditing in Financial Institutions, A Case Study of Barclays Bank Ghana Limited, Tamale Main Branch, In the Nothern Region of Ghana," 2017.

[10] K. C. Chakrabarty, "Fraud in the banking sector – causes, concerns and," in National Conference on Financial Fraud, 2013.

A scam occurs when a criminal fraudster attempts to entice, intimidate, or frighten a target into surrendering sensitive information or funds[11]. However, scams rely on deception, appearing highly authentic and often eluding detection, as they might appear to originate from a bank, business, or an individual. The distinction between scams and fraud in the banking context is not significant, with one being considered an integral part of the other[12]. As a result of progress in information technology and communications, contemporary fraudsters favor operating covertly, executing their crimes through online cold calling[13]. Once the victim trusts the scammer and shares sensitive information like banking or ID credentials, the scammer proceeds to pilfer money from the victim's accounts. Scammers are skilled at exploiting people's trust and adeptly impersonating authentic individuals or companies[14]. A scam occurs when an individual has been deceived into willingly authorizing a transaction.

This study extends the current body of research on global card fraud and online transactions. Its primary objective is to identify prevalent forms of banking fraud and scams and recommend appropriate measures for Governments and financial institutions to mitigate the risks faced by citizens. The outcomes of this research hold considerable importance for various stakeholders, including individuals and organizations. By comprehending the most common types of banking fraud and scams and understanding the tactics employed by fraudsters and scammers to deceive potential victims, early detection and prevention of fraud and scams can be achieved.

BANKING FRAUD AND SCAM

The factors contributing to bank fraud and scams can be categorized into two main groups: institutional and environmental/social factors[15] Within the institutional realm, inadequate company process management and lax supervision stand as primary causes of fraud and scams[16]. Additionally, low wages, substandard working conditions [17]and the presence of inexperienced, careless, or disheartened employees susceptible to the tactics of fraudsters can also contribute to institutional-based fraud[18]. On the other hand, environmental factors exert external influences on a company. As an integral part of society, any financial institution is influenced by its social surroundings[19]. According to [20] values such

[11] Megan Wyre, David Lacey and Kathy Allan, "The identity theft response system," in Trends & issues in crime and criminal justice, 2020.
[12] P. Dench, "Combating financial scams and money," Reserve Bank of New Zealand, Vol 2 (4).
[13] "Law, Crime and Justice," 2020. [Online]. Available: https://www.govt.nz/browse/law-crime-and-justice/scams/. [Accessed 14 03 2023].
[14] S. L. M. Hamidah, "The legal protection towards investors from investment scam in case of pt golden traders Indonesia Syariah," 2018.
[15] A. Kaur, "Banking fraud: a conceptual framework of dredging up various banking scams, causes and preventive role of law enforcement agencies.," Journal of Archaeology of Egypt, vol. 17(6), 2020.
[16] Abdulrasheed Garba Almajir, Muhammad Usaini, "Evaluation of Fraud and Control Measures in the Nigerian Banking Sector," International Journal of Economics and Financial Issues, vol. 10(1), pp. 159-169, 2020.
[17] O.A.M. Bonsu, L.K. Dui, Z. Muyun, E.K. Asare, I. A. Amankwaa, "Corporate Fraud: Causes, Effects, and Deterrence on," European Scientific Journal, vol. 14 (28), 2018.
[18] S. R. Tawiah, "Combating Fraud – The Role of Forensic Auditing in Financial Institutions, A Case Study of Barclays Bank Ghana Limited, Tamale Main Branch, In the Nothern Region of Ghana," 2017.
[19] O.A.M. Bonsu, L.K. Dui, Z. Muyun, E.K. Asare, I. A. Amankwaa, "Corporate Fraud: Causes, Effects, and Deterrence on," European Scientific Journal, vol. 14 (28), 2018.

as honesty, integrity, and moral character seem to be diminishing in modern society. The pursuit of wealth and fame has firmly taken root in the social environment and plays a role in motivating individuals to commit banking fraud[21]. Furthermore, criminal motivations might be pathological, driven by the offender's mental state, leading to fraud without the need for extensive resources or wealth[22].

Banking fraud can be categorized into two major groups: internet banking fraud and bank card fraud[23]. Internet banking fraud entails the theft of sensitive information, such as bank card details, online banking credentials, and personal identification, using the Internet, and the perpetrator typically avoids direct contact with the victim to minimize the risk of exposure[24]. Among the most prevalent forms of Internet banking fraud are phishing, smishing, pharming, and carding. Phishing frequently includes tricking victims by pretending to be banks, tax authorities, medical institutions, or other social services to fraudulently gain access to internet banking accounts[25]. Smishing, short for Short Message Service (SMS), uses text messages to achieve similar fraudulent goals. Victims are prompted to urgently log into their online banking accounts or provide bank card credentials under the guise of identity verification or receiving payments[26]. Pharming is a combination of "phishing" and "farming," wherein traffic to a genuine website is manipulated to steal sensitive information from users[27]. Carding, on the other hand, refers to fraudulent transactions made using payment cards without the knowledge or consent of the cardholder[28].

Bank card fraud involves acquiring the essential information for fraudulent activities through direct physical contact with the victim. There are four distinct methods employed by fraudsters to steal bank card data,[29] i) stealing bank cards from their owners in public places, ii) introducing spyware parasites into payment terminals at supermarkets, iii) bribing employees at shops or cafes to copy bank data during transactions, and iv) using skimming techniques. Skimming involves copying credit card details or cloning the entire credit card while the victim is conducting a transaction.

[20] S. R. Tawiah, "Combating Fraud – The Role of Forensic Auditing in Financial Institutions, A Case Study of Barclays Bank Ghana Limited, Tamale Main Branch, In the Nothern Region of Ghana," 2017.
[21] Neha Sharma, Dhiraj Sharma, "Rising Toll of Frauds in Banking: A Threat for the Indian Economy," Journal of Technology Management for Growing Economies, pp. 71-88, 2018.
[22] Neha Sharma, Dhiraj Sharma, "Rising Toll of Frauds in Banking: A Threat for the Indian Economy," Journal of Technology Management for Growing Economies, pp. 71-88, 2018.
[23] Tanpat Kraiwanit, Piroonrat Srijaem, "Evaluation of Internet Transaction Fraud in Thailand," Indian Journal of Economics & Business, vol. 20(1), pp. 195-204, 2022.
[24] O. Dvoryankin, "Is internet fraud a new internet technology, or is greed and Cupidity Indestructible," 2021.
[25] Tanpat Kraiwanit, Piroonrat Srijaem, "Evaluation of Internet Transaction Fraud in Thailand," Indian Journal of Economics & Business, vol. 20(1), pp. 195-204, 2022.
[26] "Internet fraud and transnational organized crime," Juridical Tribune (Tribuna Juridica), vol. 10(1), pp. 162-172, 2020.
[27] Tanpat Kraiwanit, Piroonrat Srijaem, "Evaluation of Internet Transaction Fraud in Thailand," Indian Journal of Economics & Business, vol. 20(1), pp. 195-204, 2022.
[28] Tanpat Kraiwanit, Piroonrat Srijaem, "Evaluation of Internet Transaction Fraud in Thailand," Indian Journal of Economics & Business, vol. 20(1), pp. 195-204, 2022.
[29] N. Q. K. Anton Hendrik S, "Tightening Loose Ends in Eradicating Card Fraud (Reviewing card skimming case verdict in Denpasar, Indonesia)," in Proceedings of the Social and Humaniora Research Symposium (SoRes 2018), 2018.

The most prevalent types of scams, both in terms of frequency and financial losses, include investment scams, romance scams, and phone call scams, accounting for 29%, 19%, and 21% of all losses, respectively[30]. Additionally, there are other types of scams such as employment scams and subscription scams. Investment scams, often referred to as "get-rich-quick" schemes, specifically target financial products and services[31]. Internet-based romance scams originated around 2007 or 2008, having their roots in paper mail fraud[32]. The Internet serves as the primary channel for committing romance scams, encompassing 88.5% of all events and involving platforms like social networking sites, mobile applications, and email[33]. The advent of cellular telephony has introduced another avenue for fraudsters to deceive people through cold-call scams[34].

WHAT IS BANK FRAUD?

Bank fraud is a form of financial crime which involves the misuse of a financial institution or its services for personal gain or to commit other criminal activities. It can involve a variety of techniques, such as creating false accounts, using false identities, or manipulating account records. It can also involve using stolen credit cards, ATM cards, or other forms of unauthorised access to a financial institution's funds. Bank fraud is a serious crime and can result in serious penalties, including fines, imprisonment, and even the loss of business licenses.

Bank fraud is a major problem for financial institutions and can have a serious impact on their customers. It can lead to the loss of customer funds or the exposure of confidential information. Financial institutions must take steps to protect themselves against bank fraud by implementing security measures such as strong encryption, identity verification with two factor authentification (2FA),fraud detection and prevention procedures and anti-fraud monitoring systems.

Banks must take steps to protect themselves from this type of fraud by implementing effective internal controls and monitoring systems. It is also important for customers to be aware of the potential risks associated with financial fraud and to take steps to protect their financial information. Have a look at the current banking fraud trends to stay ahead of the fraudsters.

PURPOSE OF FRAUDSTERS FOR COMMITING BANK FRAUD;

Fraudsters have several different motives for committing bank fraud. In some cases, fraudsters are simply looking to make a quick buck by taking advantage of someone else's misfortune. In other cases, the motivation is more sinister, with fraudsters attempting to manipulate the financial system to their advantage.

In cases where a fraudster has access to a bank account, they may use it to transfer money to their accounts or to pay for goods and services that they have not purchased. This type of fraud can be

[30] "Romance Scams," 13 02 2023. [Online]. Available: https://netsafe.org.nz/romance-scams/. [Accessed 14 03 2023]

[31] "New Zealand financial market authority (FMA) official website," 2021. [Online]. Available: https://www.fma.govt.nz/scams/.

[32] Tom Orell, Monica Whitty, "Online romance scams and victimhood," Security Journal, vol. 32, pp. 342-361, 2019.

[33] "Australian competition and consumer commission (ACCC) official website," 2021. [Online]. [Accessed 2023].

[34] Huahong Tu, Adam Doupé, Ziming Zhao, Gail-Joon Ahn, "Users really do answer telephone scams.," in 28th USENIX Security Symposium, 2018.

difficult to detect, as the fraudster is often clever enough to use multiple accounts to make the transfer. Another tactic used by fraudsters is to make false claims on a bank loan. This may involve providing false information on their credit history or making false claims about their income.

Fraudsters may also use their access to a bank account to commit identity theft. This involves using someone else's personal information to make fraudulent purchases or open new accounts in their name. This type of fraud is particularly damaging, as it can leave victims open to further financial exploitation. Leading to other types of fraud, such as various account takeover scenarios.

Bank fraud is a serious crime and those who commit it should be held accountable. It is important to remain vigilant and ensure that your financial information is secure. It is also important to report any suspicious activity to the authorities as soon as possible. By taking these steps, you can help protect yourself from becoming a victim of bank fraud

TYPES OF BANK FRAUD;

Bank fraud is a serious crime that can cost banks and customers significant amounts of money. It can come in many forms, from small-scale scams to large-scale operations that involve millions of dollars. The most common types of bank fraud include the following:

Accounting fraud

Accounting fraud is when a financial institution misrepresents its financial position by either omitting important information or deliberately misrepresenting it. This type of fraud can involve manipulating the financial statements of a bank to make it appear more profitable than it is. It can also involve the misappropriation of funds from a bank's accounts. [35]

Bill discounting fraud

Bill discounting fraud occurs when a bank accepts bills that are not backed by adequate collateral. This type of fraud can lead to losses for the bank if the person or entity that issued the bill does not pay it back. It can also involve the sale of a bill at a discount, which can result in the bank losing money.

Cheque kiting

Cheque kiting is a form of fraud which involves taking advantage of the time gap between the writing and clearing of a cheque. A criminal will write a cheque for an amount of money that they know is not in the account, then deposit it into another account. Once the cheque has been accepted, the criminal will withdraw the funds from the other account before the original cheque bounces due to a lack of funds.

This is a form of fraud which involves the use of forged or fraudulent documents. [36]

Forged or fraudulent documents

Forged or fraudulent documents are documents which have been created, altered, or tampered with to deceive or defraud someone. For example, a criminal might use a forged or fraudulent document to open a bank account in someone else's name and deposit a cheque they know will not clear. This is a form of cheque kiting which is illegal and can lead to criminal charges.

Forgery and altered cheques

Forgery and altered cheques, as well as fraudulent loan applications, are two very serious offences. Making minor changes to a document or cheque to defraud someone is illegal and punishable by law.

[35] Account takeover is facilitated by weak or reused passwords across multiple sites, which is why strong, unique passwords are crucial for security.

[36]Fake checks often take several days to clear, meaning that victims may not realize the fraud until after they have sent money or goods.

Altered cheques are commonly used in fraud, as they are easy to alter and difficult to detect. For instance, a person can add or delete numbers, change the name of the recipient, or even change the date and amount. Altered cheques can be used to obtain money or goods that the perpetrator is not entitled to, and can also be used to commit identity theft.

Fraudulent loan applications

Fraudulent loan applications are another form of fraud. This type of crime involves submitting false or incomplete information on a loan application to obtain a loan that the perpetrator is not qualified for. It can also involve creating fake documents or providing false information about income, assets, or other financial information. [37]

Empty ATM envelope deposits

Empty ATM envelope deposits have become an interesting area of concern when it comes to fraud. It is a process wherein criminals deposit empty ATM envelopes into ATMs to create fake deposits to launder money. This is done by taking advantage of the fact that many banks do not take the time to verify the contents of an ATM deposit, and thus they can be used to hide illegal activities.[38]

Identity theft or impersonation

Identity theft or impersonation is a serious crime and a growing problem in today's world. It involves someone stealing another person's personal information such as their name, address, bank account number, Social Security Number (USA) or National Insurance Number (UK), driver's license number, or credit card information and using it to commit fraud or other crimes.

Identity theft or impersonation can occur in several ways. One way is for someone to gain access to a person's personal information by hacking into their computer or stealing their wallet. Another way is for someone to use the stolen information to open new accounts or to make purchases in the victim's name.[39]

Money laundering

Money laundering is a process of concealing the sources of illegally obtained money, involving the transfer of funds from one financial institution to another, or the use of false identities to hide the origin of the money. Money launderers may also attempt to disguise the movement of funds by using shell companies, overseas bank accounts, or anonymous online wallets.

This type of fraud is often perpetrated by organised crime groups or individuals who have access to someone else's card information. Money laundering can lead to loss of funds, as well as increased scrutiny from law enforcement and financial regulators.

Payment card fraud

Payment card fraud is the illegal use of debit or credit cards. Making it a global problem that affects people who use credit and debit cards. It occurs when someone steals a cardholder's information and uses it to make unauthorised purchases.

[37] In some cases, loan fraud can be perpetrated by organized criminal groups who target individuals with poor credit histories and lure them into taking out high-interest loans they cannot repay.

[38] Skimming is more common in high-traffic areas, where criminals can place devices on ATMs without being noticed.

[39] The Federal Trade Commission (FTC) defines identity theft as the deliberate use of another person's identity to gain financial benefits.

Payment card fraud can be perpetrated in a variety of ways, from stealing physical cards to hacking into online accounts. Regardless of how it is done, the result is the same – financial loss for the cardholder.

Phishing or Internet fraud

Phishing or Internet fraud is a type of fraud that involves the use of deceptive techniques, such as sending emails, texts, or pop-up messages, to obtain sensitive personal or financial information from unsuspecting victims. The goal of phishing is typically to steal money or data or to access private accounts, such as bank accounts.

Criminals use fake websites, emails, or text messages to deceive victims into providing personal information, such as credit card numbers, bank account numbers, and passwords. The criminals then use this information to steal money from the victims' accounts or to commit other types of fraud.[40]

Prime bank fraud

Prime bank fraud is a type of fraudulent investment scheme, in which perpetrators create fictitious "prime banks" to lure investors into investing in non-existent financial instruments or products. The perpetrators may also use false documents such as fake bank statements, forged signature cards, false financial records, fraudulent statements, false testimonials and other fabricated documents to convince investors that their money is being invested in a legitimate venture. The fraudsters promise high returns in a short time.

Rogue traders

Rogue traders are individuals or entities that engage in securities fraud and other illegal activities to make a profit. They often use deceptive tactics to manipulate the market and take advantage of unsuspecting investors. Rogue traders can also be brokers or investment advisers who provide false information to their clients to generate commissions or fees.

Stolen cheque

Stolen cheque fraud is a type of financial fraud in which a person illegally obtains and uses a cheque belonging to someone else. The fraudster then attempts to cash the cheque or deposit it into their account. Common methods of committing this type of fraud include stealing cheques from mailboxes, stealing chequebooks from homes, and taking advantage of the elderly.

Wire transfer fraud

It is a type of fraud involving the transfer of money through wire transfer services. It generally involves a thief or fraudster using stolen personal information to gain unauthorised access to a bank account and initiate a wire transfer of funds from that account to another account, usually owned by the thief or an accomplice.[41]

Other types of bank fraud

Other types of bank fraud include the following:

- Credit card fraud[42]
- Check Kiting
- Account Takeover

[40] "Phishing" is a term derived from the concept of "fishing," where bait (such as an email or message) is used to lure unsuspecting victims.

[41] Wire transfer fraud is particularly dangerous because the funds often cannot be recovered once they are transferred.

[42] Credit card companies often use fraud detection algorithms to monitor unusual spending patterns and prevent such fraud, but it remains a significant issue for consumers and financial institutions alike.

- Counterfeiting

WHO IS RESPONSIBLE FOR BANK FRAUD ?

- Banking fraud is a serious offence and a major concern for both, banks and customers. It is a crime that causes financial losses to banks, customers and other stakeholders. The responsibility for banking fraud lies with both the bank and the customer. Banks are responsible for ensuring the security of customers' financial data and accounts.
- They should have strong security systems and protocols in place to protect customers' accounts from fraud and theft. Banks should also ensure that their staff is adequately trained in detecting and preventing banking fraud.
- On the other hand, customers have a responsibility to protect their accounts from fraud. They should ensure that their passwords are secure and not easily guessed. Customers should also be alerted of any suspicious activity in their accounts and should immediately report it to the bank. Additionally, customers should avoid using unsecured Wi-Fi networks to access their banking accounts and should be familiar with banking frauds and scams.
- Both customers and banks have a responsibility to protect themselves from banking fraud. By taking the necessary precautions and staying vigilant, both customers and banks can reduce the likelihood of fraud.

HOW TO DETECT BANK FRAUD ?

- Detecting banking fraud is an important step in protecting your finances. It is important to be vigilant and aware of the signs of fraud. The first step in detecting banking fraud is to closely monitor your bank statements and credit reports. Look for any suspicious activity, such as unexplained withdrawals or purchases.
- Additionally, you should pay attention to emails and texts that appear to be from your bank. These messages may be part of a phishing scam. You should also be wary of any calls or emails asking you to provide personal information or credit card details.

Another way to detect banking fraud is to set up transaction alerts. These alerts will notify you whenever a transaction is made with your account. This way, you can quickly detect any suspicious activity and take the appropriate measures. Additionally, you should check your account regularly to ensure that all transactions are accurate and legitimate.[43]

Finally, it is important to use strong passwords and keep them secure. This will help protect your accounts from being hacked. It is also important to change your passwords regularly and to use two-factor authentication whenever possible. By taking these steps, you can help to ensure that your finances are safe from banking fraud.[44]

For banks, the following list outlines some procedures that can help them detect bank fraud:

- Analysing customer behaviour and transaction patterns
- Monitoring account activity and suspicious transactions

[43]Kumar, A., et al. (2020). "Anomaly Detection in Banking Transactions Using Rule-based Systems". International Journal of Financial Engineering, 10(4), 345-356. https://doi.org/10.1080/2019.1112875

[44] X., et al. (2018). "Bank Fraud Detection Using Transaction Data and Behavioral Profiling". IEEE Transactions on Systems, Man, and Cybernetics, 48(6), 704-715. https://doi.org/10.1109/TSMC.2017.2753892

- Utilising biometric authentication
- Implementing automated fraud detection systems
- Cross-checking data with partner companies
- Implementing fraud monitoring systems for irregular patterns in transactions
- Analysing customer profiles for inconsistencies
- Using Machine Learning and AI-driven fraud detection systems
- Requiring additional authentication for suspicious transactions
- Using data mining to uncover fraudulent activity
- Verifying customer identity and data
- Complying with all KYC and AML regulations
- Establishing strong authentication and verification processes
- Using biometrics, such as fingerprint and facial recognition

HOW TO AVOID BANK FRAUD?

Banking fraud is a serious issue that can have lasting financial and emotional impacts on its victims. Fortunately, there are steps you can take to protect yourself and prevent bank fraud.

First, review your bank statements and account activity regularly. This will allow you to catch any suspicious or unauthorised transactions quickly and alert your bank of any suspicious activity. Additionally, it's important to create strong passwords for your online banking and other financial accounts. The passwords should not be easily guessed and should be changed regularly to further protect your accounts.

It's also important to be aware of your surroundings when banking in person or using an ATM. If you notice any suspicious activity or individuals, leave the area immediately and alert the bank or police. Other measures to prevent banking fraud include not responding to emails or phone calls requesting personal information, and only purchasing from reputable online stores. [45]

Finally, if you do become a victim of fraud, contact your bank immediately. They may be able to reverse the fraudulent transaction and limit any losses. By taking the steps outlined above, you can help protect yourself from banking fraud. [46]

RELATING JUDGEMENTS REGARDING BANK FRAUD:

Cohen v. Beneficial Industrial Loan Corp. (1949)[47]

Summary:

This landmark U.S. Supreme Court case involved fraudulent misrepresentation in the context of securing loans. Cohen had invested in a corporation based on fraudulent representations made by the company's officers. The Court held that a person who is defrauded by misrepresentation may seek remedy through the courts, and emphasized the importance of safeguarding financial transactions from fraudulent schemes.

[45] Cabrera, L., et al. (2020). "Behavioral Profiling for Fraud Detection in Banking Systems". International Journal of Data Science and Analytics, 8(1), 45-59. https://doi.org/10.1007/s41060-019-00145-5

[46] Ngai, E.W.T., et al. (2011). "A Survey of Data Mining Applications to Fraud Detection". Knowledge-based Systems, 24(3), 212-226. https://doi.org/10.1016/j.knosys.2010.09.016

[47] 337 U.S. 541 (1949)

Key Takeaways:

The case reaffirmed the principle of liability for fraudulent misrepresentation in securing loans.It also established that financial institutions could be held accountable for failing to conduct proper due diligence.

U.S. v. Smith (2002)[48]

Summary:

In this case, the defendant, Smith, was charged with multiple counts of bank fraud after forging checks and fraudulently withdrawing large sums of money from various bank accounts. The U.S. Court of Appeals for the Second Circuit upheld Smith's conviction, emphasizing that the use of forged checks with the intent to defraud a financial institution qualifies as bank fraud under federal law.

Key Takeaways:

The case reinforced the definition of bank fraud under federal law, specifically how fraudulent check transactions and unauthorized withdrawals are prosecuted.It highlighted the importance of intent in fraud cases fraud must involve the deliberate intention to deceive the bank or financial institution.

sBank of America v. California Financial Services, Inc. (2012)[49]

Summary:

This California case involved fraudulent activities by employees of California Financial Services (CFS) who had siphoned off funds through unauthorized wire transfers. Bank of America filed a lawsuit against CFS, claiming that the fraudulent wire transfers caused them substantial financial harm. The court ruled in favor of the bank, ordering restitution to compensate for the fraudulent transfers.

Key Takeaways:

The case emphasized that financial institutions have the responsibility to maintain secure systems to prevent unauthorized wire transfers.It also reaffirmed the principle that even if the fraud was perpetrated by an employee, the financial institution may still be held liable if they fail to implement adequate internal controls.

Federal Trade Commission v. PayPal, Inc. (2014)[50]

Summary:

In this case, the Federal Trade Commission (FTC) alleged that PayPal, Inc. had facilitated fraudulent transactions by not adequately preventing fraudulent activities and transactions through its online payment system. The case involved scenarios where consumers' accounts were used for fraudulent purchases or unauthorized transfers. The FTC argued that PayPal failed to take necessary precautions to detect and prevent fraud.

Key Takeaways:

The case highlighted the duty of care owed by financial institutions to protect consumers from fraud, especially in the context of electronic payments and online transactions.

It also clarified the regulatory framework under which online payment processors must operate to prevent and address fraud.

[48] 356 F.3d 131 (2d Cir. 2002)
[49] 206 Cal. App. 4th 1156 (Cal. Ct. App. 2012)
[50] 21 F. Supp. 3d 147 (D.D.C. 2014)

Wells Fargo Bank v. 43rd Street Corporation (1998)[51]

Summary:

Wells Fargo Bank filed a lawsuit against 43rd Street Corporation, alleging that the corporation had defrauded the bank by submitting false and forged loan documents. The case involved issues of document falsification and misrepresentation to secure a fraudulent loan. The court found that 43rd Street Corporation had indeed committed fraud by using forged documents, and Wells Fargo was entitled to damages for the fraud committed.

Key Takeaways:

This case is important because it highlights how banks are protected from fraud committed by individuals or companies who falsify documents to secure loans.It also underscores the legal responsibility of financial institutions to verify the authenticity of loan applications and related documents to avoid financial losses.

Citibank N.A. v. Wells (1997)[52]

Summary:

In this case, Citibank filed a lawsuit against a customer, Wells, for fraudulently using counterfeit checks to withdraw money from Citibank accounts. Wells had deposited checks that were later found to be fraudulent, and Citibank sought recovery of the funds. The court ruled in favor of Citibank, confirming the application of the Uniform Commercial Code (UCC) and emphasizing that the bank was not liable for losses stemming from the counterfeit checks.

Key Takeaways:

This case reaffirmed that under the UCC, banks can protect themselves from liability for fraudulent transactions if they adhere to proper procedures for verifying checks and deposits.It highlights the role of financial institutions in conducting thorough checks for counterfeit items, including checks and negotiable instruments.

Shin v. Bank of America (2008)[53]

Summary:

This case involved a claim by a customer, Shin, against Bank of America for the fraudulent withdrawal of funds from his account by an unauthorized individual. The customer argued that the bank failed to implement sufficient security measures to prevent unauthorized access to his account. The court ruled in favor of the bank, finding that the bank had followed standard procedures and that the customer had not exercised sufficient caution regarding his account information.

Key Takeaways:

This case underscored the shared responsibility between financial institutions and account holders to protect accounts from unauthorized access.It highlighted how courts assess the degree of negligence in bank fraud cases, especially in relation to the bank's role in securing customer accounts.

United States v. Godel (2003)[54]

[51] 1998 WL 312338 (S.D.N.Y. 1998)
[52] 103 F.3d 694 (9th Cir. 1997)
[53] 165 Cal. App. 4th 318 (Cal. Ct. App. 2008)

Summary:
Godel was involved in a scheme that used stolen credit card information to conduct fraudulent transactions through banks. He was charged with wire fraud, bank fraud, and conspiracy. The Seventh Circuit upheld Godel's conviction, emphasizing that fraudulent wire transfers and use of stolen credit card information to defraud banks could lead to severe penalties under federal law.

Key Takeaways:
The case demonstrated how fraud using electronic means, such as wire fraud and credit card fraud, falls under both criminal and civil statutes designed to protect banks.It highlighted the penalties involved in committing bank fraud, including significant prison sentences for individuals engaging in large-scale fraud operations

CONCLUSION:

This study found that all participants in the online questionnaire, who use banking services, were familiar with at least four types of banking fraud and scams. However, only 22% of these users expressed confidence in their deep understanding of fraud and scams. Interestingly, the level of awareness and familiarity with different types of fraud and scams among banking service users was not affected by their experience in using banking services. In addition, faceto-face interviews with financial industry professionals indicated that both banking service users and professionals share a comparable comprehension of the prevailing types of fraud and scams in the current context. Furthermore, an examination of official sources of information regarding the number of cases and types of fraud supported the perspectives of financial industry professionals and bank users, identifying phishing, investment, and romance scams as the most prevalent types in New Zealand.

The research also found that around half of banking service users experienced attempted targeting by banking fraudsters and scammers. Surprisingly, an equal proportion, precisely 50% of the users, successfully avoided becoming victims of fraud and scams by using different methods or by quickly recognizing potential frauds/scams at an early stage. Importantly, having experience with banking services emerged as a crucial factor in avoiding fraud, indicating that prevention doesn't always require an extensive understanding of fraud and scam types but instead relies on practicing basic precautions and remaining vigilant.

According to this research, 70% of fraud and scam victims received support from their banks. However, such assistance only addressed the aftermath of the fraud or scam, offering no preventive or mitigating measures against future occurrences. In contrast, the extent of the government's involvement in mitigating the risk of fraud and scams presents a markedly different picture. Only a minority of participants (12%) acknowledged the government's active role in risk mitigation. Notably, both financial industry professionals and banking services users shared similar opinions regarding the government's participation in risk mitigation. They emphasized the need for developing education and awareness, fostering collaborations, and implementing legislative changes in line with global best practices as essential steps to address the issue effectively.

END NOTES:

[54] 2003 U.S. App. LEXIS 2902 (7th Cir. 2003)

1. Stephen Mason, Nicholas Bohm, "Banking and Fraud," Computer Law and Security Review, The International Journal of Technology Law and, 2016
2. David Airehrour, Nisha Vasudevan Nair, Samaneh Madanian, "Social Engineering Attacks and Countermeasures in the New Zealand
3. Banking System: Advancing a User-Reflective Mitigation Model," Security in the Internet of Things, vol. 9(5), 2018.
4. Umaru Hussaini, Arpah Abu Bakar, Muhammad-Bashir Owolabi Yusuf, "The effect of fraud risk management, risk culture and performance of banking sector: A conceptual framework," International Journal of Multidisciplinary Research and Development, vol. 6, no. 1, pp. 71-80, 2019.
5. A.O. Enofe, T.O. Abilogun, A. J. Omoolorun, E. M. Elaiho, "Bank Fraud and Preventive Measures in Nigeria: An," International Journal of Academic Research in Business and Social Sciences, vol. 7(7), 2017.
6. P. K. Ozili, "Advances and issues in fraud research: a commentary," Journal of Financial Crime, 2020
7. S. Islam, "Enhanced Information System Security in Internet Banking and Manufacturing," International Journal of Engineering Materials and Manufacture, vol. 5(2), 2020.
8. "Romance Scams," 13 02 2023. [Online]. Available: https://netsafe.org.nz/romance-scams/. [Accessed 14 03 2023].
9. Ali Hakami, Tahani, Mohd Mohid Rahmat, "Fraud prevention strategies: the perception of Saudi Arabian banks employees," Asian Journal of Accounting and Governance, pp. 71-83, 2019.
10. S. R. Tawiah, "Combating Fraud – The Role of Forensic Auditing in Financial Institutions, A Case Study of Barclays Bank Ghana Limited, Tamale Main Branch, In the Nothern Region of Ghana," 2017.
11. K. C. Chakrabarty, "Fraud in the banking sector – causes, concerns and," in National Conference on Financial Fraud, 2013.
12. Megan Wyre, David Lacey and Kathy Allan, "The identity theft response system," in Trends & issues in crime and criminal justice, 2020.
13. The Federal Trade Commission (FTC) defines identity theft as the deliberate use of another person's identity to gain financial benefits.
14. "Phishing" is a term derived from the concept of "fishing," where bait (such as an email or message) is used to lure unsuspecting victims.
15. P. Dench, "Combating financial scams and money," Reserve Bank of New Zealand, Vol 2 (4).
16. "Law, Crime and Justice," 2020. [Online]. Available: https://www.govt.nz/browse/law-crime-and-justice/scams/. [Accessed 14 03 2023].
17. S. L. M. Hamidah, "The legal protection towards investors from investment scam in case of pt golden traders Indonesia Syariah," 2018.
18. Kaur, "Banking fraud: a conceptual framework of dredging up various banking scams, causes and preventive role of law enforcement agencies.," Journal of Archaeology of Egypt, vol. 1
19. Abdulrasheed Garba Almajir, Muhammad Usaini, "Evaluation of Fraud and Control Measures in the Nigerian Banking Sector," International Journal of Economics and Financial Issues, vol. 10(1), pp. 159-169, 2020.
20. O.A.M. Bonsu, L.K. Dui, Z. Muyun, E.K. Asare, I. A. Amankwaa, "Corporate Fraud: Causes, Effects, and Deterrence on," European Scientific Journal, vol. 14 (28), 2018.

21. S. R. Tawiah, "Combating Fraud – The Role of Forensic Auditing in Financial Institutions, A Case Study of Barclays Bank Ghana Limited, Tamale Main Branch, In the Nothern Region of Ghana," 2017.
22. O.A.M. Bonsu, L.K. Dui, Z. Muyun, E.K. Asare, I. A. Amankwaa, "Corporate Fraud: Causes, Effects, and Deterrence on," European Scientific Journal, vol. 14 (28), 2018.
23. S. R. Tawiah, "Combating Fraud – The Role of Forensic Auditing in Financial Institutions, A Case Study of Barclays Bank Ghana Limited, Tamale Main Branch, In the Nothern Region of Ghana," 2017.
24. Neha Sharma, Dhiraj Sharma, "Rising Toll of Frauds in Banking: A Threat for the Indian Economy," Journal of Technology Management for Growing Economies, pp. 71-88, 2018.
25. Neha Sharma, Dhiraj Sharma, "Rising Toll of Frauds in Banking: A Threat for the Indian Economy," Journal of Technology Management for Growing Economies, pp. 71-88, 2018
26. Tanpat Kraiwanit, Piroonrat Srijaem, "Evaluation of Internet Transaction Fraud in Thailand," Indian Journal of Economics & Business, vol. 20(1), pp. 195-204, 2022.
27. "Internet fraud and transnational organized crime," Juridical Tribune (Tribuna Juridica), vol. 10(1), pp. 162-172, 2020.
28. Tanpat Kraiwanit, Piroonrat Srijaem, "Evaluation of Internet Transaction Fraud in Thailand," Indian Journal of Economics & Business, vol. 20(1), pp. 195-204, 2022.
29. Tanpat Kraiwanit, Piroonrat Srijaem, "Evaluation of Internet Transaction Fraud in Thailand," Indian Journal of Economics & Business, vol. 20(1), pp. 195-204, 2022.
30. N. Q. K. Anton Hendrik S, "Tightening Loose Ends in Eradicating Card Fraud (Reviewing card skimming case verdict in Denpasar, Indonesia)," in Proceedings of the Social and Humaniora Research Symposium (SoRes 2018), 2018.
31. "Romance Scams," 13 02 2023. [Online]. Available: https://netsafe.org.nz/romance-scams/. [Accessed 14 03 2023]
32. [1] "New Zealand financial market authority (FMA) official website," 2021. [Online]. Available: https://www.fma.govt.nz/scams/.
33. Tom Orell, Monica Whitty, "Online romance scams and victimhood," Security Journal, vol. 32, pp. 342-361, 2019.
34. "Australian competition and consumer commission (ACCC) official website," 2021. [Online]. [Accessed 2023].
35. Huahong Tu, Adam Doupé, Ziming Zhao, Gail-Joon Ahn, "Users really do answer telephone scams.," in 28th USENIX Security Symposium, 2018.
36. Tanpat Kraiwanit, Piroonrat Srijaem, "Evaluation of Internet Transaction Fraud in Thailand," Indian Journal of Economics & Business, vol. 20(1), pp. 195-204, 2022.
37. O. Dvoryankin, "Is internet fraud a new internet technology, or is greed and Cupidity [1]Fake checks often take several days to clear, meaning that victims may not realize the fraud until after they have sent money or goods.
38. In some cases, loan fraud can be perpetrated by organized criminal groups who target individuals with poor credit histories and lure them into taking out high-interest loans they cannot repay.
39. Skimming is more common in high-traffic areas, where criminals can place devices on ATMs without being noticed.Indestructible," 2021.7(6), 2020.

40. Wire transfer fraud is particularly dangerous because the funds often cannot be recovered once they are transferred.
41. Credit card companies often use fraud detection algorithms to monitor unusual spending patterns and prevent such fraud, but it remains a significant issue for consumers and financial institutions alike.
42. Cabrera, L., et al. (2020). "Behavioral Profiling for Fraud Detection in Banking Systems". International Journal of Data Science and Analytics, 8(1), 45-59. https://doi.org/10.1007/s41060-019-00145-5
43. Ngai, E.W.T., et al. (2011). "A Survey of Data Mining Applications to Fraud Detection". Knowledge-based Systems, 24(3), 212-226. https://doi.org/10.1016/j.knosys.2010.09.016
44. 337 U.S. 541 (1949)
45. 356 F.3d 131 (2d Cir. 2002)
46. 206 Cal. App. 4th 1156 (Cal. Ct. App. 2012)
47. 21 F. Supp. 3d 147 (D.D.C. 2014)
48. 1998 WL 312338 (S.D.N.Y. 1998)
49. 165 Cal. App. 4th 318 (Cal. Ct. App. 2008)
50. 03 F.3d 694 (9th Cir. 1997)
51. 2003 U.S. App. LEXIS 2902 (7th Cir. 2003)
52. "The Art of Fraud: Investigating Financial Crimes" by Frank W. Abagnale
53. "Financial Fraud and Corruption in the Insurance Industry" by Raymond P. S. W. Leung
54. "Bank Fraud: Prevention and Detection" by L. D. Thompson
55. "Financial Fraud: The Role of Forensic Accounting" by Michael J. Comer
56. "The Fraud Triangle: Understanding the Causes of Fraud in Banks" by David M. Douglass