Migration Letters

Volume: 20, No: S11(2023), pp. 28-36

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Protecting Bank Customers from Cyber Threats (Electronic Fraud and Identity Theft) and the Legal Guarantees Introduced in Saudi Legislation

Nesreen Madah Aburaya[1], Dr. Shemseddine Ethani Barnat[2]

Abstract

With the increasing reliance on digital banking services, protecting bank customers from cyber threats such as cyber fraud and identity theft has become a critical concern. This paper explores the legal safeguards introduced by Saudi legislation to protect the interests of bank customers and enhance cyber security measures. It studies the basic provisions and regulations established by the Saudi authorities to combat cyber threats and ensure the protection of customer data and financial transactions. The study also addresses the role of financial institutions in implementing these legal guarantees and the collaborative efforts between banks and regulatory bodies to create a safe banking environment. By analyzing the current legal framework and its effectiveness, this research contributes to a comprehensive understanding of the measures applied to protect bank customers in the Kingdom of Saudi Arabia and provides insights into potential areas for improvement and access to the laws adopted by Saudi legislation to protect personal data and secure user privacy.

Keywords: *cyber threats, electronic fraud, identity theft, legal, Saudi legislation.*

Introduction

Modern technologies have proven to be a double-edged sword in the banking sector, as the banking sector has clearly benefited from intensive efforts to combat electronic fraud from modern technologies, as the transition from the monetary system to transferring funds electronically can lead to a reduction in the risks of money embezzlement and a decrease in money holdings, as well as the development of methods and tools for detecting fraud due to advanced technology tools (Al-Radfani, 2014)

On the other hand, fraudsters excelled in using electronic technologies and employing them to enhance their capabilities, which made it easier for them to defraud easily and to have a superior and high ability to communicate with other technologies, penetrate information, and access data, as various document technologies allowed forgery and embezzlement practices, and it is difficult to discover them, as the methods of forging checks were previously simple. It was replaced by high-quality counterfeiting of all negotiable securities, including checks (Al-Maqsoudi , 2017).

[1] Assistant professor at Imam Abdulrahman Bin Faisal University, Applied College, nmaburaya@iau.edu.sa
[2] Assistant professor at Imam Abdulrahman Bin Faisal University, Applied College, chebarnat@iau.edu.sa

Modern technologies have also led to the risk of traditional fraud associated with insider trading operations, causing a high risk of exposure to financial losses. When a bank employee fraudulently changes the status of the debt or when a broker conducts unapproved transactions or exceeds the transaction limits, each of them causes exposure. (Al-Otaibi, 2021) The bank is exposed to potentially devastating losses for a short period of time, in addition to the fact that switching to banking activity through the Internet exposes banks to new risks, as fraudsters are deeply familiar with the latest technologies, in addition to the weak points that lie in the banks' internal control procedures, and this represents a risk of cybercrime Rising (Al-Shehri Ali, 2019).

Concept of electronic fraud and identity theft

Electronic fraud refers to the practice of fraud by relying on the use of the Internet and digital means. It often depends on the Internet, and this use involves deceptive methods in which individuals or organizations are deceived so that financial gains are achieved. It is possible for electronic fraud to take a number of forms. Various types, such as electronic phishing, are carried out through a fraudulent attempt to obtain sensitive information such as login credentials, credit card details, or social security numbers by masquerading as a trustworthy entity through electronic communication such as email messages or fake websites. (Al-Shammari, 2016)

Or spoofing (which is the act of disguising communications from an unknown source as coming from a trusted entity, for the purpose of tricking recipients into revealing sensitive information or committing fraudulent acts) and identity theft that occurs (with the unauthorized use of another person's personal information, such as name or phone number). Social Security or financial account details so that fraudulent activities are committed to obtain financial benefits). Electronic fraud is a series of fraudulent schemes and practices that are conducted through the Internet, such as advance fee fraud, pyramid schemes, or fake markets through the Internet and individuals are deceived into providing money or sensitive information under false pretenses (Al-Shazly, 2020).

With reference to the reality of electronic fraud in the Saudi business environment, statistics have shown that (20%) of Saudi citizens are exposed to cases of fraud and fraud through applications and websites, and (3 billion dollars) losses from fraudsters impersonating the personalities of senior executives in major well-known companies, and (203) people were exposed to electronic fraud in the world, (20%) of the most common cases, (71%) of identity thefts, (66%) of phishing cases, and (63%) of account thefts. As for the losses of merchant retail worldwide due to electronic fraud, losses in 2011 reached 9.84 billion dollars, and there has been a (45%) increase in fraud operations since 2017. As for 2020, losses reached 32.4 billion dollars, and losses in 2027 are likely to reach about 40.6 billion dollars. (Al-Khudary, 2020)

As for identity theft, it is one of the types of fraud in which an individual's personal information is stolen and used without his consent for various harmful purposes. It is possible to use the stolen information to conduct unauthorized transactions or open fraudulent financial accounts, as well as to apply for credit, loans, or participation in other criminal activities. Identity theft can cause major financial loss and damage to a person's credit history. Several common methods for identity theft include data breaches, in which unauthorized access is made to the database or systems that contain it. (Luna, 2016, p7)

Personal information and similar information lead to the disclosure of sensitive data to cybercriminals, or social engineering, which is carried out by manipulating individuals through psychological tactics to extract personal information or unauthorized access to accounts and systems.

Types of Fraud

Symptoms of the decline of internal controls include the possibility of electronic fraud in banks, as symptoms of internal control include a weakness in the control environment, a

lack of segregation of duties, a lack of financial guarantees, weak independent checks and balances, a lack of appropriate licenses and appropriate documents and records, and an overflow of current controls with insufficient accounting systems.

(AGWU, M. EDWIN, 2014, P177) indicates that environmental factors increase the possibility of embezzlement, such as insufficient rewards, insufficient internal controls, a lack of separation of duties or audit trails, in addition to ambiguity in job roles, duties, responsibilities, and areas of accountability, and perhaps personal performance and behavior are at less than acceptable levels.

Associated with insufficient operational audits and a lack of timely or periodic review and inspection to ensure compliance with company objectives, priorities, policies, and government regulations to implement policies related to honesty and loyalty.

First: Internal fraud: It is the construction of the relationship between the perpetrator and the bank, such that the fraud is classified as external or internal (internal is committed by the customer or a third party) or internal (it is committed by employees or management), and in the case of cooperation between internal and external parties, the fraud is classified As internal. (AGWU, 2014)

Based on the goal and intention that are classified as credit, the goal is to obtain financing, the underlying intention is not to pay or to be extravagant, and the intention is to never pay. Based on a number of cases in which electronic fraud was committed for each crime perpetrator who has no connection to other operations or multiple ones based on an organized attack or group of fraudulent operations linked to one person who committed the crime.

Second: Friendly fraud is also known as civil fraud or family fraud: This type is committed using information related to a trusted friend or an individual, and to the extent that financial institutions, independent organizations, and the media inform consumers of the necessity of not sharing confidential data, Many people share their personal information with close friends or family members, and statistics have recently indicated an increasing percentage of those exposed to cases of identity theft through personal impersonation, such as when the customer contacts the bank or financial institution because he cannot access his account through the Internet, and while speaking with a call service representative, the representative can see someone logging into the customer's online account, and when he asks if anyone knows the private password, the customer explains that he shared it with one of their family members and the password is the same as the password for the ATM machine and accordingly. An individual can steal money without the will of its owner. (Keneilwe, 2019)

Third: Identity theft: This is done when an individual’s identity is hidden by using another person’s identity through a filter. The source of identity is often forged, such as a driver’s license or passport. Identity theft is known as a widespread phenomenon in banking fraud through the Internet, and this matter has received a great deal of attention from the media, as it has become a source of concern for many consumers. Identity theft can be simple or complex, depending on the contact information of a collection agency. This comes after some research was conducted, as the thief steals and opens many credit cards according to current accounts in various banks and passes invalid checks so that they reach the victim’s account via the Internet and transfer the money by paying the bill. Here, the customer receives a notification of a returned check in the mail and contacts customer service to discover that sums of money have been deducted from his account. Research reveals that the account number was used to postpone purchases through the Internet (Michael, 2018).

FRAUD PREVENTION STRATEGIES

Fraud includes a huge group of illegal operations that are carried out intentionally through betrayal or misrepresentation. Fraud perpetrators engage in deceptive acts to

obtain a financial or moral benefit without incurring any costs. Financial fraud is one of the operations that cannot be underestimated because of its far-reaching repercussions in various matters. Fields such as institutions and companies, specifically banks, and because financial and operational losses arise from unrealized gains due to high expenses, this causes psychological difficulties. The organization's reputation, good faith, and relationship with customers are most affected by fraudulent activities, and the increase in fraudulent activities in the recent past has affected the business environment in the Kingdom of Saudi Arabia, as the current measures taken are consistent with preventing and detecting fraud, but they are still ineffective (Rehman, 2015).

Studies have examined fraud prevention strategies by individual researchers, anti-fraud organizations such as ACFE, and professional accounting and auditing bodies. Fraud prevention methods have taken various forms of techniques that are taken in two ways: (Al-Shawabkeh, 2019)

First, the strategies that are implemented in the pre-employment stage so that the applicant’s status and history are examined

Second: Measures taken during the recruitment period to prevent fraud

In the reports submitted by certified fraud examiners, many fraud prevention strategies are revealed that have proven effective and confirm that fraud prevention methods can reduce the chances of fraud occurring and are less expensive than detection.

The nature of cyber threats facing banks

The nature of the threat is considered one of the most serious challenges facing financial institutions and banks, as the prevailing and potential threats in the field of cyber security stem from several sources, as they take the form of sabotage activities targeting individuals, companies, and the national infrastructure of countries, and the effects of these threats cause major risks, the most important of which is harm to public safety and harming the security of the state and the stability of the international community. (Al-Sanea, 2020)

The real problem lies in the possibility of concealing the malicious use of information technology. It is difficult to determine the origin or identity of the criminal, and even the motive behind the crime is not easy to discover. It is also possible for threat actors to operate with great freedom from almost anywhere, and it is possible that the motives for hacking are related to showing ingenuity. Simply put, technology steals money and information. Criminals pose a threat to the state and have been considered a threat, as hackers use different types of harmful tools and methods in addition to taking criminal activities in new and innovative forms on a daily basis.

- Easily erase and destroy evidence.

The second problem comes in the ease with which evidence is erased and destroyed by the perpetrator in a short period, in addition to the ease with which he evades the criminal act, as the most important challenges facing cyber security and hindering the processes of proof in the field of modern cybercrimes are the concealment and concealment of crimes most of the time, to the point that the victim may not be aware of the existence of the cybercrime that occurred against him, as well as the perpetrator's ability to conceal the behavior that constituted his crime and to obscure its features through the invisible manipulation of electronic pulses or oscillations (Al-Samhan, 2020, p44).

- Banking hack

The bank is hacked by relying on various methods that can be exploited by the threat actor to penetrate the bank.

This is done by using weak encryption suites such as SSL/TLS from web applications, seizing accounts to command and control them, and using affected peripheral devices such as external USB devices. (Al-Samhan, 2020, p45)

Use perimeter and weak controls for antivirus defense and gain full access to and control over private banking websites.

Perhaps the common weakness that hackers and attackers exploit is internal employees or people who have interacted with or have prior knowledge of banking systems.

Anti-Cybercrime Law in the Kingdom of Saudi Arabia

The laws in the Kingdom of Saudi Arabia are governed by Islamic Sharia. Sharia consists of a set of political principles derived from various sources. These sources are the Holy Qur'an and the Sunnah of the Prophet.

Forbidden acts are forbidden according to Sharia law and are punished with specific punishments stipulated in the Holy Qur'an. If the Qur'an and Sunnah are silent about them, then here comes the role of the judge in using his discretion to determine the appropriate punishment. It is possible that the punishments include imprisonment, cash compensation, or deprivation of some rights, and while determining the severity Punishment The judge takes into consideration compensation for the harm caused to the victim and whether this harm is actual or consequential. However, only actual compensation proven by Saudi judicial bodies is awarded. (Al-Qahtani, 2011)

The modern Arab Convention on Combating Electronic Crimes (No. 126 of 2012) was approved in the Kingdom of Saudi Arabia. This agreement mainly addresses the rise in cybercrime and includes credit card fraud, cyberthreat, fraud, electronic forgery, piracy, system interference, access, and illegal interception. It also aims to encourage cooperation between Arab countries in the area of combating cybercrime. (Al-Qahtani, 2011)

The agreement also stipulated the importance of enforcing the copyright law, and penalties were imposed on violators of the terms and regulations of the agreement. The Kingdom of Saudi Arabia had previously issued a cybercrime penalty system consisting of sixteen articles.

Personal data protection law

The Personal Data Protection Law (PDPL) was approved based on a royal decree issued on September 16, 2021, approving Resolution No. 98 on September 4, 2021. The Saudi Data and Artificial Intelligence Authority (SDAIA) is tasked with enforcing the new legislation within two years. The first two, after which consideration was given to transferring supervision to the National Data Management Office (NDMO), which is the regulatory part of SDAIA, So that the Personal Data Protection System and its enforcement regulations are established as a legal basis for protecting the rights of customers, in accordance with what relates to the information processing of personal data through parties in the Kingdom, in addition to the inclusion of parties abroad that carry out the information processing of personal data of residents of the Kingdom through the use of personal data processing relying on the Internet (Al-Sheti, 2019).

a. Data interoperability regulations

The Saudi government has officially addressed the interoperability framework since 2006 in accordance with a national digital strategy for the Saudi government.

The development was also based on interoperability and includes shared data and technical standards based on (Yesser) frameworks for interoperability, the purpose of which is to allow ministries and government agencies to implement their roles by exchanging information and presenting it through the integrated common infrastructure, as the excellent facilitation of providing electronic services easily with coordinated technical features makes operability a high priority based on digital transformation plans,

The treatment focused on an existing interoperable plan that includes the following: (Al-Sheti, 2019)

- Defining common data standards at the business and logical levels Data schemas describe the structures used to communicate between systems.

- Standards are defined for metadata, attributes, and dictionaries that are used to index electronic content.

- It includes technical standards and policies with interoperability at the technical level and includes communication and networking standards, integration standards, and security.

B. Data policies relating to data sharing

There is no storage of data for an individual alone, as its content, structure, and storage must be accompanied by other information. It must also include information and instructions regarding mandatory issues for the validity of the data used. Examples of this are that the stored information must be determined according to the duration of data storage or its validity, which requires specifying a period of time. Whenever data becomes outdated, it should never be shared, which is known as data retention It includes: (Al-Khudary, 2020)

- Legal references and links to the official legal source

- Updated data and schedule to update frequently.

- Protected and controlled access.

- The shared data should be flexible in use, direction, or capture for individual analysis or report generation.

All personal data is directly related to the objectives of (GOV.SA) so that it does not conflict with the legal texts that have been established, in addition to the necessity of providing tools and means to collect personal information in a way that suits the customer's special circumstances directly and in safe ways that are devoid of any misleading means, as it is clear that all personal data is not necessary to fulfill the purpose, and GOV.SA ceases to store or destroy previously obtained and collected data (Al-Sheti, 2019).

e. Data management and usage policies

Privacy, data protection, and regulations covering data protection in the Kingdom have been accepted and understood by the authorized user. All data platforms require that all data platforms have the ability to control the platform and its applications. In addition, the agreement enters into force immediately after using the platform or accessing it the first time it is used (Al-Sheti, 2019).

All personal data is directly linked to aspects of digital government, such as providing online services in an easier and more efficient manner, so that it does not conflict with the terms of regulations and data privacy and security policies, and so that the multiple methods used in all personal information must be appropriate to the owner's circumstances and may be direct. It is clear and free from deception, misrepresentation, and blackmail. All information is no longer necessary to achieve the purpose of its capture and storage by the competent authority so that it stops hoarding and destroying the data that was previously collected immediately, and the following standards are verified by the digital government (GOV.SA) for all personal data: (Al-Qahtani, 2011)

- Justifications for all personal data
- The purpose of all personal data, whether complete or partial, mandatory or optional, shall be accompanied by more information about the processing of data that does not conflict with the purpose of its collection or what is stipulated by law.
- Identity and reference address for all personal data when appropriate for security purposes.
- The entities to which the personal data will be disclosed and a description of whether the personal data will be transferred, disclosed, or processed outside the Kingdom
- The other elements are determined according to the regulations based on the nature of the activity practiced by the bank.

Cyber security legislation

The Cyber security Protection Law consists of the following:

Anti-Cybercrime Law: The purpose of the Anti-Cybercrime Law is to define crimes and determine their penalties, and its purpose is to ensure information security, protect the public interest and morals, protect the rights to legitimate use of computers and information networks, and protect the national economy.

National Cyber security Authority (NCA): The National Cyber security Authority has issued a number of controls and guidelines related to cyber security at the national level to enhance cyber security in countries in a way that protects their vital interests, national security, and the vital infrastructure of government services. It also includes controls and legal frameworks of guidance issued by the body, which include: (Al-Shazly, 2020)

- Data cyber security controls.
- Cyber security controls for critical systems.
- Operational controls.
- Saudi Cyber security Workforce Framework (SCyWF)
- National Coding Standards (NCS)
- Saudi Cyber security Higher Education Framework (SCyber-Edu)

Freedom of information regulations

Freedom of information in the Kingdom is one of the most prominent information policies that is emphasized, as the necessity of a policy of the right of access to information related to confidential public information has been stressed, in addition to the necessity of demarcating eligibility controls for requesting information and the individual's right to obtain it, as obtaining information is limited. Platforms have the right for civilians to apply for it and provide contact information for relevant parties to communicate to answer inquiries regarding freedom of information. Freedom of public information that is confidential or not protected is concerned with processing by the platform, regardless of its source or natural form, and open data that is included in the framework. For public information, it is called the process of providing individuals with general data in exchange for a free information fee, or what is known as the policy of the right to obtain relevant information (Al-Shazly, 2020).

Conclusion

In conclusion, the Kingdom of Saudi Arabia has implemented several legal procedures to protect bank customers from cyber threats and identity theft. These measures include the

Cybercrime Law, data protection regulations, the use of two-factor authentication, secure online banking platforms, fraud monitoring systems, and consumer education initiatives. (Al-Otaibi, 2021) These legal frameworks and security measures aim to ensure the integrity of online transactions, safeguard customer information, and deter electronic fraud. However, it is essential for bank customers to remain vigilant, adopt best security practices, and promptly report any suspicious activities to their banks and local authorities to enhance their protection against cyber threats and identity theft. (Al-Maqsoudi, 2017)

The Kingdom has taken systematic measures to protect bank customers and has also worked to introduce laws related to artificial intelligence and cyber threats. The Saudi Data and Artificial Intelligence Authority (SDAIA) has assumed responsibility for supervising data protection regulations in the country, as these regulations require banks and financial institutions to implement strong security measures to protect customer data and prevent unauthorized access, disclosure, or misuse (Al-Shehri Ali, 2019).

In addition, two-factor authentication is widely adopted by Saudi banks to enhance the security of online transactions, as customers are usually required to provide an additional authentication factor, such as a one-time password (OTP) sent via SMS or generated by a mobile application, in addition to their login credentials. (Al-Qahtani, 2011)

providing platforms for secure online banking services. It is obligated to provide secure online banking platforms with strong security features, as these platforms use encryption techniques, Secure Socket Layer (SSL) certificates, and firewalls to protect customer data and transactions from interception or unauthorized access. Banks have also used advanced fraud monitoring systems to detect and prevent fraudulent activities. These systems use algorithms and machine learning techniques to identify suspicious transactions or patterns, which helps mitigate potential risks and protect customers from financial losses.

Saudi banks cooperate closely with law enforcement agencies to combat cybercrime, providing the necessary information and support during investigations to identify and arrest cybercriminals involved in fraud or identity theft.

References

Al-Radfani Muhammad, (2014) Police investigations in the face of cybercrime challenges, Arab Journal for Security Studies, Volume 31, Issue 61

Al-Maqsoudi Muhammad, (2017) Information Crimes, Al-Arabiya Journal for Faithful Studies, Volume 33, Issue 7

Al-Otaibi Ziad, (2021) Cybercrimes committed via digital media, International Arab Journal for Legal Studies, Volume 3, Issue 1

Al-Shehri Ali, (2019) A strategic vision to reduce cybercrime to enhance cybersecurity in the Kingdom of Saudi Arabia, College of Strategic Sciences, Naif Arab University for Security Sciences

Ghanem Al-Shammari, (2016) Information Crimes, International Scientific House, first edition, Amman.

Al-Shazly Fattouh, (2020) Organized Ta'zir Crimes in the Kingdom of Saudi Arabia, Al-Rushd Library, Fourth Edition, Riyadh.

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. Technology and Health Care, 24(1), pp.1-9.

AGWU, M. EDWIN (2014), REPUTATIONAL RISK IMPACT OF INTERNAL FRAUDS ON BANK CUSTOMERS IN NIGERIA, International Journal of Development and Management Review (INJODEMAR) Vol. 9, No 1

Keneilwe Zuva, Tranos Zuva (2019) Hack the Bank and Best Practices for Secure Bank Trust Tshepo Mapoka, Cyber Security Centre of Excellence (CSCE),Vol.7 pp. 17-21

Michael.A. Dennis. (2018).” Cybercrime”, Selected by Britannica Academic, Encyclopedia Britannica, PP. 1-51.

Mayer. Jonathan. (2016) Cybercrime litigation, University of Pennsylvania Law Review, 164 U. Pa. L. Rev. 10521 -1453.

Rehman, H.,Masood ,A.& Cheema ,A.(2015). Information Security Management in Academic Institutes of Pakistan,2nd. National Conference of Information Assurance(NCIA)

Al-Shawabkeh, Adnan Awad. (2019). The role of information security procedures in reducing information security risks at Taif University, Journal of Studies and Research, Volume (11), Issue (4), 164-187.

Al-Sanea, Noura Omar; Asran, Awtaf Saad Al-Din; Al-Sawat Hamad bin Hamoud bin Humaid; Abu Aisha, Zahida Jamil Nimr; Suleiman, Enas Al-Sayyid Muhammad. (2020). Teachers' awareness of cybersecurity and ways to protect students from Internet risks and enhance their national values and identity, vol. 36, no. 6, 41-90.

Al-Samhan, Mona Abdullah. (2020). Requirements for achieving cybersecurity for administrative information systems at King Saud University, Journal of the College of Education, Mansoura University, No. 111.

Al-Qahtani, Salem bin Saeed, Al-Anzi, Hamoud bin Muhammad. (2011): Information exchange between security agencies in the Kingdom of Saudi Arabia: A field study, doctoral thesis, Department of Police Sciences, College of Graduate Studies, Naif Arab University for Security Sciences, Saudi Arabia.

Al-Sheti, Enas Muhammad Ibrahim. (2019). Evaluating information security and privacy policies in educational institutions in the Kingdom of Saudi Arabia: An applied study on Qassim University, the Egyptian Society for Information Systems and Computer Technology, Cairo.

Al-Khudary, Jihan Saad Muhammad; My regards, Hoda Jibril Ali; Kulaibi, Nima Nasser Madbash. (2020). Cybersecurity and artificial intelligence in Saudi universities: a comparative study, Journal of University Performance Development, Vol. 12, No. 1, October, 2020 2735-3222.