Romblon State University Research Journal
ISSN: 2619-7529 (Online) | ISSN: 2350-8183 (Print)
Volume 6 (2): 28—36, 2024

Computer System Evaluation: Information Security for Electronic Money Transfer Services

Preexcy B. Tupas[1] and Alexander Hernandez[2]

ABSTRACT

This research examines how various organizations address the security challenges associated with money transfer systems. It reveals that the role of payment systems in money transfers has significantly evolved, with numerous electronic payment systems now available to facilitate secure online transactions. The study also identifies key success factors for each organization implementing its security solutions. Rapid technological advancements pose substantial risks to transaction security. The research shows that payment systems have become increasingly integral to the industry, and their impact on society is considerable. These advancements are expected to benefit future studies by offering insights into technological progress in both monetary and digital transactions. A range of sources, including academic journals, conference proceedings, and online articles, were used to review the current landscape of money transfer systems thoroughly. The study emphasizes the critical role of security measures and customer awareness in safeguarding electronic payment systems. Its findings offer valuable insights for policymakers, financial institutions, and researchers working on effective security strategies for money transfer systems.

Keywords: *Money Transfer System, risk for security, success factors, security practices and processes*

INTRODUCTION

Money transfer transactions have been a subject of continuous interest as individuals transfer funds to and from various locations. Camara (2016) critically examines remittances within a typical social context, highlighting that remittances reflect strong social bonds between migrants and their families left behind in their home country. Money transfer services for domestic and international transactions are transitioning from conventional providers to digital platforms, aiming to capture market share through enhanced accessibility and more affordable options (Merritt, 2011). These evolving services have played a key role in driving economic growth, directly and indirectly, by streamlining payment processes and trade and generating substantial revenue for the service providers.

✉ : ptupas@rsu.edu.ph
[1]Romblon State University, College of Computing, Multimedia Arts and Digital Innovation;
[2]Technological Institute of the Philippines- Manila
Received 14 January 2024; Revised 3 September 2024; Accepted 16 December 2024

The rapid advancements in technology present significant risks in maintaining the security and reliability of electronic money transfer systems in today's digital landscape (Seetharaman & Raj, 2011). A major challenge for developers of electronic payment systems is ensuring both security and privacy, as digital information can be susceptible to breaches during transmission or while stored on servers (Aghdami, 2012). According to Grabner-Kräuter and Faullant (2008), many potential users avoid online money transfers due to privacy concerns, necessitating security improvements to build client trust and acceptance. Gaber et al. (2016) suggest that Security Information and Event Management (SIEM) systems could address these issues. However, these systems are currently more suited for network monitoring and need enhancements in multi-layer security, scalability, and resilience. Effective solutions are required to reliably and promptly detect fraud across various channels that handle daily transactions.

This review tries to fill this learning gap by better understanding the underlying processes and practices of different companies with electronic money transfer systems to have a strong intellect of security. Specifically, this study addressed the following research questions: (a) what are the practices and processes of the

company to provide security in their transactions?; and (b) what are the success factors involving the technology used in providing security?

To explore these issues, the paper investigates four organizations involved in money transfer payment systems, focusing on their methods for managing data and transaction security. It examines the strengths and weaknesses of each organization through a qualitative approach and various case studies. These companies exemplify common practices in executing transactions within the money transfer system. The Philippines was chosen as a case study due to its representation of typical features of developing countries, particularly in the ASEAN region (Karanasios, 2008). Light and Lewandowski (2015) report that remittance inflows to the Philippines increased from $1.46 billion in 1990 to $26.7 billion in 2013, with projections of $28.4 billion for 2014. In 2013, remittances accounted for 9.3 percent of the national GDP. According to the International Monetary Fund, the Philippines ranked third in total remittances worldwide in 2012, with total official payments (classified by the IMF as BPM6) amounting to $26 billion, surpassed only by China and India. This research is anticipated to provide valuable insights for other developing nations with similar technological, socio-economic, civic, cultural, and legal contexts as the Philippines. Currently, no comprehensive study addresses the factors, practices, and processes related to the security of money transfer systems in the Philippines.

Related Works

Background of Money Transfer System

Money Transfer Definition. Bogdan (2015) defines payment as transferring something valuable from one party to another in exchange for goods or services or to fulfill a legal obligation. Historically, payment systems have progressed from the simplest barter system—where goods or services are directly exchanged—to modern methods such as E-cash and electronic payment systems. Today, traditional payment methods for individuals include cash, checks, debit cards, credit cards, bank transfers, and online payments.

The SWIFT network (Society for Worldwide Inter-Bank Financial Telecommunication), which became operational in 1977, is a global payment system that allows banks to automate international payments, statements, and other banking communications (Bogdan, 2015). Operating in over 200 countries, SWIFT is the largest international payment network, encompassing more than 10,000 financial institutions. It offers a secure and dependable platform for cross-border transactions, facilitating global financial operations such as payments to international employees and contractors. Although SWIFT is not a bank or financial institution, it serves as a messaging platform for banks to transmit transaction information. Based in Belgium, SWIFT ensures secure financial communications for its member institutions.

Banks like First Bank and United Bank for Africa use the SWIFT system to receive international money transfers in Nigeria. However, these banks cannot send funds abroad due to regulatory constraints. The functionality of electronic fund transfers within Nigeria heavily relies on the use of local area networks (LAN) and wide area networks (WAN) (Ekwueme et al., 2011). Koskosas (2011) highlights that electronic fund transfers offer significant benefits to clients, including greater convenience and reduced transaction costs. However, these advancements also present new challenges for banks, particularly in maintaining the financial system's security.

Trends and Risks of Money Transfer System. Tools, methods, and principles are necessary to transfer assets among participants. This constitutes a payment system to ensure that financial transactions are completed reliably, securely, efficiently, effectively, and accessibly (Mbuguah & Karume, 2013). Payment systems all have hazards, yet they endeavor to utilize electronic store exchange. Risks for Payment systems involve:

Legal: The risk of loss arises when legal frameworks do not support the system's rules and contracts cannot be enforced.

Credit: The risk that a counterparty fails to meet their obligations fully.

Liquid: In countries where non-bank entities issue e-cash, regulators often address concerns by requiring these issuers to maintain liquid assets equivalent to the total value of customer deposits (i.e., the total and outstanding electronic value issued, referred to as "e-float"). The risk here is that a counterparty may not fulfill its obligation on time but might settle later (DuPont, 2019).

Operational: The risk that human errors, malicious attacks, or deficiencies in the IT infrastructure could lead to financial losses.

Systemic: The risk of one participant's failure to meet their obligations could trigger a chain reaction affecting the entire financial system.

Reputation: The risk that the payment system's inability to meet its requirements effectively and reliably may result in a loss of trust from clients and counterparties.

The authors suggest that while these risks have been present in traditional payment systems, they are even more critical in electronic fund transfers, especially within Internet banking (DuPont, 2019).

In recent years, the banking sector has made considerable progress in electronic communication with customers, driven by the increasing number of Internet users. This advancement in electronic distribution channels has enhanced customer access to banking products and services. However, it has also introduced new risks, such as the potential for data breaches, unauthorized account access by hackers, and theft of customer funds. Securing electronic banking systems is a major challenge for bank management worldwide, as evidenced by numerous successful attacks on commercial banks and their clients. An essential part of tackling this issue involves raising customer awareness about security measures and potential threats (Belás et al., 2015).

Proposed Security Measures for Money Transfer. Security is a critical issue in business banking and is associated with various activities. Ensuring banking security involves multiple factors, as business bank security is a complex system encompassing various elements such as capital management about credit, market, and operational risks (i.e., capital adequacy policies). Effective security measures focus on operational risk, defined as the risk of loss resulting from internal processes, human errors, or external conditions (Grubicka, 2015).

In recent years, the rate of cybercrime has gradually increased. These criminal activities target digital security and data and invade personal information through electronic banking systems. Many criminals penetrate banking databases by breaching security measures to steal clients' personal details (e.g., account information, card details, user IDs, passwords) illegally. Once criminals obtain this personal information, client accounts become vulnerable to attacks. This poses a risk not only to customers but also to the banks themselves. Common authentication methods, including passwords, user IDs, identification cards, and PINs, face several limitations. Passwords and PINs can be unlawfully acquired through direct observation or other illicit methods (Islam, 2015).

The Internet Banking Customer Satisfaction Model

The IBCS (Internet Banking Customer Satisfaction) model identifies six key components: content, accuracy, order, ease of use, timeliness, and security. This model emphasizes that internet security is a critical factor for customers. The study by Chen et al. (2012) reveals that content and order significantly influence customer satisfaction, highlighting their prominence within the IBCS model. The relative importance of the other components is ranked as follows: accuracy, ease of use, timeliness, and security. This ranking suggests that content, order, accuracy, and timeliness are crucial for providing access to sensitive financial information through Internet banking. Additionally, ease of use and security are important areas where banks should focus their investments to attract customers to their e-services. Customers generally expect a user-friendly interface and robust security measures for online transactions.

Encryption and Decryption. E-money transfer is vulnerable to attacks by hackers who use different malware and viruses to alter the transferee information and the transfer amount. According to Al-hamami et al. (2012), there are three main phases and layers of solution for fraud prevention: (1) Lock the browser, (2) Encryption, and (3) Decryption. These solutions are combined to provide the best results in preventing fraudulent attacks. The study found that the banking side plays a significant role in the detection process by checking whether the transaction process successfully transferred the amount efficiently and without error or inquiring about any failures from both the bank and customer sides.

Today, many customers prefer making electronic payments instead of cash or checks in person or via mail. Various electronic payment systems have been developed to facilitate secure Internet transactions. To ensure the security of these transactions, two cryptographic techniques are utilized as part of electronic payment frameworks. One technique is used to encrypt and decrypt the transmission to the recipient, while the other is a public key infrastructure that involves both a private and a public key (Camenisch et al., 2015).

Biometric-based authentication and identification systems

Biometric-based validation and identification systems are emerging as effective solutions to address the security and privacy challenges anticipated in the coming years. Biometrics offers a viable approach for automatically identifying individuals based on their physiological or behavioral characteristics, providing a better solution for the growing security demands of our information society. As biometric sensors become more affordable, the public will likely recognize biometrics as an effective method to prevent fraud, making this technology increasingly prevalent in transactions requiring authentication (Fatima, 2011).

Practices and Solutions for Different Types of Money Transfer Methods

These days, the most utilized electronic installment frameworks are the accompanying Smart card-based e-installment framework, Online segment framework, Mobile telephone-based layer framework, E-Wallet Payment System, and E-Check Payment System. New payment types are continuously discovered, and additional methods are continually developed yearly.

Smart card-based electronic payment system

The smart card is a plastic card embedded with an integrated circuit chip, providing users with flexibility and data portability. It combines features of plastic and magnetic cards used for various identification purposes into a single card, allowing access to multiple services, networks, and the Internet. This versatility enables its use in numerous functions and applications (Sumanjeet, 2009).

Online payment system

Online payments, which depend on Internet banking, involve transferring funds or purchasing through the Internet. Customers can transfer money to third parties from their bank accounts or use credit, debit, and prepaid cards for online purchases. The online payment system enables clients of financial institutions to perform financial transactions on secure websites managed by these institutions, which may include retail banks, virtual banks, credit unions, or building societies (Uddin & Akhi, 2014).

Mobile Phone-Based Payment System

Goyal et al., (2012) explored how mobile phones can be used for various transactions. Consumers can make payments by sending SMS messages, entering PINs, and using WAP for online transactions. Alternatively, they can manage different aspects of their transactions via their mobile devices. With advancements in communication technologies, it is anticipated that consumers will soon be able to use infrared, Bluetooth, NFC, and other technologies to transmit complete transaction data, enabling secure and efficient payments directly from their mobile devices. These mobile devices include smartphones, PDAs, wireless tablets, and other gadgets that connect to the mobile network to facilitate transactions.

Money Transfer Mechanism

In the remittance transfer process, beneficiaries receive cash through a remittance company, which ensures that recipients can collect their money from one of the company's branches or affiliated networks. Remittance transfers are prevalent in the Philippines, where the industry is advanced and competitive. Key aspects of the remittance payment process include:

Database Creation: The database may be simple, containing only names, the amount sent, and tracking numbers. However, banks may request additional information. Providers typically require an Excel file format for system uploads (Poisson, 2011).

Identification and Authentication: Remittance companies require official identification, listing 19 acceptable forms, including voter identity cards and barangay certificates, to withdraw cash. They may also accept NGO IDs (excluding banks). At the point of payment, recipients must present the tracking number and provide a signature. Procedures are in place to assist illiterate recipients and to handle minor discrepancies between the declared name and ID spelling, as long as these do not alter the recipient's gender. Significant discrepancies prompt contact with the agency for guidance.

Currency: Cash or e-money provided through G-cash can be used as the voucher.

Point of Payment (PoP): Payments can be made at the provider's branch or through a partner network location (e.g., a store). Some providers establish temporary PoPs in areas without existing facilities.

Reporting and Reconciliation: Electronic reporting and reconciliation are available daily or in real-time, with an audit trail that complies with financial and anti-money laundering regulations.

Promotion, Training, Communication, and Customer Support: Beneficiaries receive a brief session to obtain their tracking number and understand the pick-up process. Providers are developing communication materials and offering customer support through a call center for efficient complaint resolution. Technical assistance, such as an account manager, may be provided to work with NGOs.

The remittance process is typically quick, straightforward, and cost-effective, although the aid agency may face challenges as it needs to generate a separate order for each beneficiary. This payment method is designed to be user-friendly and convenient for recipients, especially those less familiar with complex systems. However, beneficiaries are required to visit a branch to collect their funds.

METHODOLOGY

This study employs a multiple case study methodology (Dubé & Paré, 2003; Yin, 2003) combined with a qualitative interview approach (Myers & Newman, 2007) to assess security measures in selected companies and to promote a reliable system mechanism. Interviews are structured interactions between interviewers and respondents, shaped by the specific contexts and conditions in which they occur (Fontana & Frey, 2000). The study aims to thoroughly investigate how each company's money transfer system operates to understand how they implement safety solutions against threats. Qualitative interviews are a prevalent and crucial tool for data collection in qualitative research (Rubin & Rubin, 2005).

The use of multiple case studies involving different types of organizations using similar types of a payment system in their money transfer is precious for this study.

Table 1. The participants for multiple case study

Company	Classification of remittance	Designations
A	International	Supervisor, Operator,
B	Local	Software Maintenance, Operator
C	International	Supervisor
D	Local	Operator

There should be a development of a more wide-range understanding of the implementation, particularly concerning the practices and processes of their solutions for security. Multiple case studies are favored over single case studies because findings from multiple cases generally provide more robust conclusions than those from a single case alone (Yin, 2003). This rationale underpins the decision to use a multiple-case study approach in our research. Regarding the use of qualitative interviews, Schostak and Barbour (2005) note that this method allows for in-depth exploration of a specific topic, offering insight into the meanings that interviewees attribute to the subject matter.

Several companies using money transfer system transactions between the Philippines and other international remittance centers were selected for the multiple case study. There is an equal presentation of local and international remittance centers to compare their transactional mechanism. Presented in Table 1 is a brief descriptor of the interviewees from the four cases. Interviews were conducted with the first participants concerned with the money transfer mechanism within the cases. This study employed semi-structured open-ended questions during the interviews and documented them upon full consent and agreement of the members.

This study also involved transcribing interviews to perform multi-level qualitative analysis, aiming to deeply understand the content through systematic coding and identifying themes or patterns (Hsieh & Shannon, 2005). Neuman (2007) defines a unit of analysis as an individual, a group, an organization, or a particular aspect of social life under investigation. This concept is crucial for data collection and analysis, including observation, empirical measurement, and concept development. In this research, four companies are utilized as the units of analysis, providing a range of money transfer system mechanisms that serve as the foundation for adequately addressing the research questions.

This study addresses consistency by following the guidelines Yin (2003) and Neuman (2007) established. To ensure construct validity, four techniques are employed: triangulation through multiple sources of evidence, comprehensive literature reviews on relevant topics, and having interviewees review the case study reports. These methods collectively ensure the accuracy of transcription and translation, and they establish a chain of evidence through a case study repository. External validity is addressed using the replication logic technique, which enhances the generalizability of the study's findings. Internal validity is ensured through the careful selection of cases and interviewees, rigorous data collection procedures, and the appropriate application of theory and literature to explain the money transfer system and remittance phenomena. The internal validity is tested to confirm that the identified causal relationships are broadly applicable.

To ensure reliability in this review, a contextual analysis approach is used for data collection, a case study repository is employed to store all research data, and a pilot study is conducted to validate the interview questions. Neuman (2007) recommends the use of a pilot study as a method to enhance the reliability of measures. Two preliminary reviews were conducted with remittance centers to assess the feasibility of examining the research topic across various organizations using money transfer systems.

RESULTS AND DISCUSSION

The following describes the practices and processes for securing transactional methods for each company's money transfer system, as well as the success factor of each company in implementing these transactions.

Transaction Controls

To prevent the network from being exploited for unauthorized payments, various controls are implemented:

A. Real-Time Transaction Controls: The company employs advanced transaction controls designed to restrict the amount of funds and the number of transactions in areas known for high levels of human smuggling.

B. Transaction Monitoring and Regulatory Reporting: Transactions are continuously monitored to detect suspicious activities and to meet regulatory reporting requirements.

C. Interdiction and Blocking: In collaboration with law enforcement, efforts are made to block individuals suspected of illegal activities from accessing the service.

Prevention of Fraud

Although technology offers numerous advantages, it also presents increased opportunities for fraudsters to deceive individuals through email, websites, and phone calls. Scams can target anyone, including those seeking companionship, aspiring lottery winners, online shoppers, and job seekers. To combat these fraudulent activities and stay ahead of emerging scams, companies adopt a multifaceted strategy: enhancing consumer

awareness, providing training for their agents or operators, investing in advanced technological solutions, and collaborating with law enforcement agencies.

A. Engaging their agents and operators in proper training against fraud.

Agents receive training to recognize potential fraud victims. If an agent suspects a transaction may be fraudulent, they are instructed to refuse or report it for further investigation. As frontline representatives in customer service, agents are equipped with various tools and techniques to prevent fraud. This support includes access to training resources and materials such as fraud kits, newsletters, fraud alerts, and an online Agent Resource Center.

According to Company C (Branch Supervisor):

"Our company offers training for agents to recognize signs of consumer fraud and authorizes them to decline transactions they suspect are fraudulent. We also run a reward program, the Eagle Eye Award, to recognize agents who successfully identify and prevent fraud. Additionally, we monitor agent performance and review consumer fraud complaints to assess whether agents require further training, additional oversight, or potential disciplinary actions such as suspension or termination. These evaluations have improved our programs, including enhanced transaction controls and increased training and support where necessary."

B. Investing in Fraud-Prevention Technology

Senders often prioritize finding the most cost-effective and convenient method when transferring money. As a result, the reliance on physical infrastructures is decreasing, with many money transfer services exploring new technologies like the Internet and mobile phones as viable alternative channels. A typical process for these transactions involves sending SMS notifications to inform recipients of the control number generated by the system.

According to the Company A (Supervisor):

"Our system technology plays a crucial role in enhancing our security measures. We use various system controls to monitor transaction activities, ensure thorough consumer due diligence, and comply with legal and internal recordkeeping and reporting requirements. Many of these controls are activated when transactions reach certain currency thresholds."

C. Fraud prevention through identification and authentication

For receiving transactions, the receiver must provide a valid ID for identification. Fail to provide such identification, cannot access their transaction. This aims to identify the profile of the receiver properly.

According to Company Operator/Agent (Company B):

"There must be a proper credentials and proof of the profile of the receiver to allow us to identify them that they are the right person to receive the money."

According to Company Operator/Agent (Company D):

"We make sure that we deliver the money to the right person by asking them to provide valid ID's or NSO Birth certificate."

Empowering Consumers through Information

A. Pricing and Transparency

Various external stakeholders consider pricing a critical factor. When evaluating pricing, it is essential to provide solutions for small and medium-sized businesses, universities, and other organizations, including options for bill payments and cost-effective prepaid cards. However, consumer-to-consumer money transfer services often attract the most scrutiny regarding pricing.

According to Company C (Branch Supervisor):

"To ensure consumers can make well-informed decisions, we offer several methods for disclosing fees and foreign exchange rates. Our agents provide this information at the point of sale prior to completing the transaction, and senders receive a receipt detailing both the fees and exchange rates associated with their transaction."

B. Transparency in Marketing

The company is committed to adhering to all regulatory obligations, which include implementing appropriate security measures to safeguard personal information from unauthorized access and misuse.

C. Data Security and Privacy

The Privacy and Records Management team is tasked with developing policies to protect consumer information. The handling of personal data is governed by privacy regulations that can vary by country and, within a country, by state.

The standard procedure for remittance transfers across companies involves several key steps. First, the sender provides the funds and recipient information. The remittance company or the sender then issues a tracking number to the recipient. Finally, the recipient can collect the cash from any branch by presenting the tracking number and a valid ID.

The process further includes contracting with a remittance company, funding the company account, setting up a bank account, and uploading a recipient list. The tracking numbers provided to recipients facilitate the pick-up process and communicate relevant details to them.

In the Philippines, remittance transfers are prevalent, and the industry is characterized by sophistication and competitiveness. Agencies utilize this method for secure cash transfers, with the company managing the disbursement and ensuring discretion by conducting transactions in closed branches at the recipient's convenience.

Key operational considerations include ensuring branch accessibility, although some providers offer mobile remittance services or temporary points for cash distribution. Recipients present their tracking numbers and ID at the branch, where the provider disburses the cash, offers customer support, and maintains communication with the agency. Reports on withdrawals are provided daily or in real-time. This method is typically fast, simple, and cost-effective. However, setup and contracting processes may be prolonged, particularly if remittance providers lack experience working with humanitarian agencies. Despite this, the system is designed to be user-friendly for recipients, though it requires them to visit a branch.
The results indicate that the remittance transfer process is streamlined to enhance convenience and security. Tracking numbers and ID verification ensure that only authorized recipients can access the funds, which aligns with best practices in financial security, as noted in the literature (Al-hamami et al., 2012). This method also leverages existing branch networks to facilitate cash distribution, reflecting a practical approach to remittance that balances efficiency with accessibility.

The prevalence of remittance transfers in the Philippines highlights the industry's adaptation to local needs and competitive dynamics. According to Poisson (2011), tracking numbers and recipient identification are crucial for preventing fraud and ensuring accurate disbursements. This is consistent with findings from previous studies that emphasize the importance of secure and transparent processes in financial transactions (Chen et al., 2012; Sumanjeet, 2009).

Despite the need to travel to a branch, the convenience of the remittance process for recipients underscores the system's effectiveness in providing reliable and secure cash transfers. However, the challenges associated with setup and contracting, particularly for humanitarian agencies, suggest that further improvements could enhance the system's efficiency. These findings align with the observations of Belás et al. (2015), who noted that improving operational aspects and streamlining interactions with different types of organizations can further optimize remittance services.

The study's results confirm the effectiveness of the remittance transfer process while also identifying areas for potential improvement. The combination of technological and procedural measures ensures security and efficiency, although the integration with humanitarian agencies could benefit from additional support and streamlined processes.

CONCLUSION

The research was conducted, designed, analyzed, and interpreted independently, primarily focusing on examining security processes and practices in money transfer systems in the Philippines. It provides a detailed look at the technological and procedural measures selected companies adopt. It offers insights into how these systems operate, their impact on consumer trust, and implications for future research and practice. There are no conflicts of interest related to this study, and it was conducted without financial or personal relationships influencing the outcomes. Ethical research practices were strictly followed, including obtaining informed consent from all interview participants and ensuring their confidentiality and anonymity. The study complied with relevant ethical guidelines and institutional review board requirements, maintaining integrity and respect for participants' rights.

This study focuses on the security processes and practices adopted in the money transfer systems within the Philippines, offering insights valuable to academic and professional fields. Initially, the study outlines the mechanism of money transfer systems, providing background information on the systems under review. It then details the processes and practices of selected companies using these systems, emphasizing how their security implementations and transaction controls contribute to their effectiveness in providing reliable cash transfer services.

The findings offer significant insights into these systems' operations and the various methods used to secure transactions, including technological and external strategies. This understanding aids consumers in developing trust in their chosen payment systems. Moreover, the study is beneficial for payment system operators, as it underscores the importance of continuous process improvement, staying updated on emerging trends and risks, and devising effective solutions to address them.

Moreover, the interviews conducted in this study reveal that the money transfer payment systems have significantly evolved within the industry. Future research could explore how these systems impact society by advancing technology in monetary transactions and promoting paperless transactions. Given that our study involves a multiple case study of four organizations, it is important to interpret the findings within their contexts. The study prioritizes a detailed understanding of the experiences of the participating organizations over statistical generalization. Notably, the case study participants have effectively adopted digital advancements, enhancing the security and efficiency of their money transfer systems.

AUTHORS' CONTRIBUTIONS

The authors confirm equal contribution to the paper.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

REFERENCES

Aghdami, S., & Khorsandi, S. (2010, April). Secure and anonymous TTP-based Electronic Payment Systems and making anonymity and security via multi-user interfaces and passwords. In *2010 2nd IEEE International Conference on Information Management and Engineering* (pp. 359–364). IEEE.

Al-hamami, A. H., Najadat, F. A. O., & Wahhab, M. S. A. (2012). Web application security of money transfer systems. *Journal of Emerging Trends in Computing and Information Sciences, 3*(3), 365–372.

Belás, J., Korauš, M., Kombo, F., & Korauš, A. (2016). Electronic banking security and customer satisfaction in commercial banks. *Journal of security and sustainability issues, 5*(3), 411–422.

Bogdan, A. (2015). Security issues and solutions in e-payment systems. *Urs Fiat Iustitia, 1*.

Camara, S. S. (2016). Remittance market of Finland: Case study of personal remittance transmission. [Unpublished Master's Thesis] Häme University of Applied Sciences.

Camenisch, J. L., Piveteau, J. M., & Stadler, M. A. (1994). Security in electronic payment systems. *Institute for Theoretical Computer Science, ETH Zurich. In: Proceedings of the ESO RISKS, 94*.

Chen, R. F., Hsiao, J. L., & Hwang, H. G. (2012). Measuring customer satisfaction of Internet banking in Taiwan: scale development and validation. *Total Quality Management, 23*(7), 749–767. https://doi.org/10.1080/14783363.2012.704284

Dubé, L., & Paré, G. (2003). Rigor in information systems positivist case research: Current practices, trends, and recommendations. *Management Information Systems Quarterly, 2003*, 597–636. https://doi.org/10.2307/30036550

DuPont, Q. (2019). *Cryptocurrencies and blockchains*. John Wiley & Sons.

Ekwueme, C. M., Ph.D., Egbunike, P. A., Ph.D., & Amara Okoye, Msc (2011). An Empirical Assessment of the operational efficiency of electronic banking: Evidence of Nigerian banks. *Review of Public Administration & Management, 1*(2).

Fatima, A. (2011). E-banking security issues-Is there a solution in biometrics?. *Journal of Internet Banking and Commerce, 16*(2), 1.

Fontana, A., & Frey, J. (2000). H.(2000). The interview: From structured questions to negotiated text. *The Handbook of Qualitative Research*, 733-768.

Gaber, C., Gharout, S., Achemlal, M., Pasquet, M., & Urien, P. (2012, May). Security challenges of mobile money transfer services. In *Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SARSSI)*.

Goyal, V., Pandey, U. S., & Batra, S. (2012). Mobile banking in India: Practices, challenges and security issues. *International Journal of Advanced Trends in Computer Science and Engineering, 1*(2).

Grabner-Kräuter, S., & Faullant, R. (2008). Consumer acceptance of internet banking: the influence of internet trust. *International Journal of Bank Marketing, 26*(7), 483-504. https://doi.org/10.1108/02652320810913855

Grubicka, J., & Matuska, E. (2015). Sustainable entrepreneurship in conditions of UN (Safety) and technological convergence. *Entrepreneurship and Sustainability Issues, 2*(4), 188.

Hsieh, H. F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research, 15*(9), 1277-1288. https://doi.org/10.1177/1049732305276687

Islam, S. H., Khan, M. K., & Li, X. (2015). Security analysis and improvement of 'a more secure anonymous user authentication scheme for the integrated EPR information system'. *PloS One, 10*(8), e0131368. https://doi.org/10.1371/journal.pone.0131368

Karanasios, S. (2008). An e-commerce framework for small tourism enterprises in developing countries

[Unpublished doctoral dissertation] Victoria University.

Koskosas, I. (2011). E-banking security: A communication perspective. *Risk Management, 13*, 81-99. https://doi.org/10.1057/rm.2011.3

Light, M. K., & Lewandowski, B. (2015). *The Impact of Western Union Agent Locations: A Case Study of Remittances in the Philippines.* University of Colorado.

Mbuguah, S., & Karume, S. (2013). Trends in Electronic Money Transfer in Kenya. *Journal of Emerging Trends in Computing and Information Sciences, 4*(1), 1857-7881.

Merritt, C. (2011). Mobile money transfers services: The next phase in the evolution of person-to-person payments. *Journal of Payments Strategy & Systems, 5*(2), pp 143-160.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization, 17*(1), 2–26.

Neuman, W. L. (2007). *Basics of social research*. Pearson Education, Inc.

Poisson, G., CaLP, 2011. *Cash transfer programming in emergencies: Cash transfer mechanisms and disaster preparedness in the Philippines*. The Cash Learning Partnership.

Rubin, H. J., & Rubin, I. S. (2005). *Qualitative interviewing: The art of hearing data (2nd Ed*.). Sage.

Barbour, R. S., & Schostak, J. (2005). Interviewing and focus groups. *Research Methods in the Social Sciences, 1*(1), 41-48.

Seetharaman, A., & Raj, J. R. (2009). Evolution, development and growth of electronic money. *International Journal of E-Adoption (IJEA), 1*(1), 76-94. https://doi.org/10.4018/jea.2009010106

Sumanjeet. (2009, November). Emergence of payment systems in the age of electronic commerce: The state of art. In *2009 First Asian Himalayas International Conference on Internet (pp. 1-18)*. IEEE.

Uddin, M. S., & Akhi, A. Y. (2014). E-wallet system for Bangladesh an electronic payment system. International *Journal of Modeling and Optimization, 4*, 216-219.

Yin, R. K. (2009). *Case study research: Design and methods (Vol. 5).* Sage.