Unlocking Financial Inclusion in Trinidad and Tobago Through Electronic Funds Transfer

Unlocking Financial Inclusion in Trinidad and Tobago Through Electronic Funds Transfer

By

Don Charles

Cambridge
Scholars
Publishing

Unlocking Financial Inclusion in Trinidad and Tobago
Through Electronic Funds Transfer

By Don Charles

This book first published 2025

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN: 978-1-0364-1754-3
ISBN (Ebook): 978-1-0364-1755-0

TABLE OF CONTENTS

PREFACE

The objectives of this study are to: i) review the international landscape for best practices regarding electronic funds transfer (EFT); ii) conduct a diagnostic assessment of the current state of EFT policy for Trinidad and Tobago (T&T); iii) empirically determine if EFT can have a positive contribution and impact on economic activity in T&T; iv) provide recommendations for an EFT framework for T&T.

The transfer entropy from the proxy variable for EFT to the real GDP was 0.7824, suggesting that in the historical data of the EFT process, 0.7824 bits of information contribute to predicting the subsequent value of real GDP. This suggests that a causal relationship exists from EFT to T&T's real GDP.

When the dependence was measured between T&T's real GDP and the EFT proxy, a Student-t Copula found a dependence of 0.6962. The results suggest that there is a moderate and positive relationship between EFT and T&T's real GDP.

When a wavelet decomposition was used to decompose each time series into details, the results found a strong dependence at the approximation level. But weak dependence at the higher frequency details. This provides evidence that in the long-run, EFT has a strong positive effect on T&T's real GDP. Therefore, development of the enabling environment for EFT should lead to increases in T&T's real GDP.

Several recommendations were made for the development of policy measures to increase EFT in T&T. Notable recommendations include:

1. Developing a Payment Systems Act which should encompass all aspects of payment systems. It should i) establish a clear regulatory authority, such as the Central Bank of Trinidad and Tobago, with the responsibility for overseeing all payment systems operations; ii) produce detailed operational standards for payment systems; iii) include a component on consumer protection; iv) regulate emerging technologies; and v) incorporate anti-money laundering and counter financing of terrorism provisions to ensure that payment systems are not used for illicit activities.

2. Developing a financial regulatory sandbox framework that allows financial technology companies and other financial service providers to test new products, services, and business models in a controlled and supervised environment.
3. Fully proclaim the Data Protection Act to allow for the protection of people's data.

Keywords: Electronic funds transfer; cybersecurity; payment systems; financial inclusion; Trinidad and Tobago

1. INTRODUCTION

Electronic payments have revolutionized the way financial transactions are conducted, encompassing all methods that eliminate the need for physical cash or paper transactions. Since the advent of automated teller machines (ATMs), debit card systems such as LINX, and credit cards in the 1990s, individuals and businesses have enjoyed the convenience of conducting transactions electronically. One of the key components facilitating these transactions is Electronic Funds Transfer (EFT), which enables the seamless transfer of funds between accounts and financial institutions through computer networks. EFT has become a cornerstone of modern banking, offering efficiency, speed, and accessibility to users worldwide, ultimately reshaping the landscape of financial services.

Electronic payments are being prized for being fast, secure, and allowing the precise transfer of funds between parties. However, this is only possible through a dependable clearance and settlement system. Clearance entails validating that the payer has adequate funds for the transaction and that the payment method is legitimate, while settlement involves transferring the actual value from the payer to the beneficiary or recipient of the funds. Clearance must be finalized before settlement to guarantee a seamless transaction process. The clearance and settlement processes play a crucial role in mitigating the risk of insufficient funds, fraudulent transactions, and errors, thereby maintaining the security and reliability of electronic payments.

Adopting electronic payments offers numerous benefits for a country, as it significantly enhances efficiency, reduces bureaucracy, and strengthens competitiveness in the global marketplace. By transitioning to electronic payment systems, governments can streamline financial processes, reducing the time and resources required for traditional paper-based transactions. This efficiency not only enhances overall productivity but also reduces administrative burdens and costs associated with manual processing. Also, electronic payments enable faster and more transparent transactions, improving the speed and accuracy of financial transactions.

The Government of the Republic of Trinidad and Tobago (GORTT) has long recognized the importance and positive aspects associated with digitalization and adopting electronic payments. Subsequently, in 2009, the

GORTT launched a project called the "Single Electronic Window (SEW) for Trade and Business Facilitation". A key component of the project is TTBizLink, which is an online platform that furnishes individuals and businesses with information related to the government's digital services related to trade and business.

The TTBizLink platform has two key components. The first is the Trinidad and Tobago Trade and Business Information Portal, which as its name implies provides information to the public. The second component is the SEW Government E-Services, which allows for payments for various government services.[1]

Despite the notable advancements in digitalizing services and facilitating electronic payments, the GORTT remains committed to enhancing the country's enabling environment for electronic funds transfer. To this end, the GORTT aims to strengthen the policy framework and the legal and regulatory infrastructure governing EFT systems. Additionally, efforts will be directed toward promoting financial inclusion and leveraging the latest

[1] By April 2024, the SEW Government E-Services allowed payments for i) the Ministry of Agriculture (MoA) Animal Production and Health Division animal import permit and animal export permit; ii) ExporTT's Certificate of Origin for Preferential Markets; iii) the Food and Drugs Inspectorate's Export Free Sale Certificate, Export Health Certificate, Goods Declaration Processing; iv) the Ministry of Trade and Industry's Investment Directorate's fiscal incentives and import duty concessions; v) the Ministry of Works and Transport Maritime Services Division's Pre Arrival Notice (Navigational aid dues) and Pre Departure Notice; vi) the Ministry of Health Pesticides and Toxic Chemicals Inspectorate's Pesticides Premises Licence, Toxic Chemicals Premises Licence, Pesticides Import Licence, Toxic Chemicals Import Licence, Toxic Chemicals Drawdown Certificate, Toxic Chemical Export Licence, Goods Declaration Processing; vii) the Ministry of Health Pharmacy/Drug Inspectorate's Antibiotics Storage, Sale and Distribution Licence, Narcotics Storage, Sale and Distibution Licence, Antibiotic Import Licence, Narcotics Import Licence, Antibiotics Withdrawal Certificate, Narcotics Withdrawal Certificate, Antibiotics Export Licence, and Antibiotics Withdrawal from Bond Certificate; viii) the Ministry of Agriculture Plant Quarantine Services's Plant Import Permit, Goods Declaration Processing; ix) the Ministry of Trade and Industry Trade Licence Unit's Trade Import Licence, Trade Export Licence, Duty Relief Licence, Safeguard Certificate, Suspension Certificate, Goods Declaration Processing; x) Trinidad and Tobago Bureau of Standards (TTBS) Goods Declaration Processing, xi) Trinidad and Tobago Chamber of Industry and Commerce (TTCIC) Certificate of Origin for Non-Preferential Markets; xii) Ministry of National Security Work Permit Secretariat, Work Permit - Individual application, and Work Permit - Group application (GORTT, 2024).

technologies to optimize the efficiency and accessibility of electronic payment services. However, there are lurking threats to the EFT industry such as cybersecurity risks and fraud. Therefore, a comprehensive approach is required.

1.1 Objective

The objective of this study is to enhance the policy and legislative framework for electronic funds transfer in T&T.

1.2 Sub-objective

The sub-objectives of this study are to:

- Review the international landscape for best practices regarding EFT.
- Conduct a diagnostic assessment of the current state of EFT policy in Trinidad and Tobago (T&T).
- Empirically determine if EFT can have a positive contribution and impact on economic activity in T&T.
- Provide recommendations for an EFT framework for T&T.

This study is structured as follows. Section 2 presents a literature review on electronic funds transfer, covering topics such as the payment system, digital payments, and cross-border payments. cyber security threats, and the importance of financial inclusion. Section 3 delves into the regulatory landscape governing payments, while Section 4 ventures into the issues regarding cybersecurity. Section 5 explores the issues surrounding consumer protection. Section 6 dives into the issues of financial inclusion. Section 7 explores the policy and legal framework specific to electronic funds transfer in T&T. Section 8 offers policy recommendations. Section 9 concludes this study.

2. WHAT IS ELECTRONIC FUNDS TRANSFER

Before delving into electronic funds transfer, first a discussion is made about a country's national payment system. This discussion is provided in the following subsection.

2.1 The National Payment System

The payment system comprises all arrangements and institutions facilitating the exchange of value between payers and payees within a financial system. This encompasses various payment instruments, such as checks and payment cards, each associated with specific payment arrangements. Together, these arrangements form the national payment system of a country. Payment and settlement systems, on the other hand, are mechanisms established to facilitate the clearing and settlement of financial transactions, ensuring secure, affordable, and accessible payment services that promote economic development and financial stability (Summers, 1994).

The national payment system serves as the backbone of a country's financial infrastructure, facilitating the transfer of funds between individuals, businesses, and government entities. It encompasses various payment instruments, payment channels, clearing and settlement mechanisms, cross-border payments, and regulatory oversight.

Payment instruments are the methods used to initiate and authorize transactions. These include cash, checks, credit cards, debit cards, and electronic funds transfers. Cash, which is a physical form of currency, is a commonly used medium for transactions. It is used for in-person transfers and can be physically saved to measure value and store value. Checks are paper documents instructing a bank to transfer funds from the payer's account to the payee's account. Credit and debit cards allow individuals to make purchases using funds directly withdrawn from their bank account. EFTs enable electronic transfers of funds between accounts, often initiated through online banking applications.

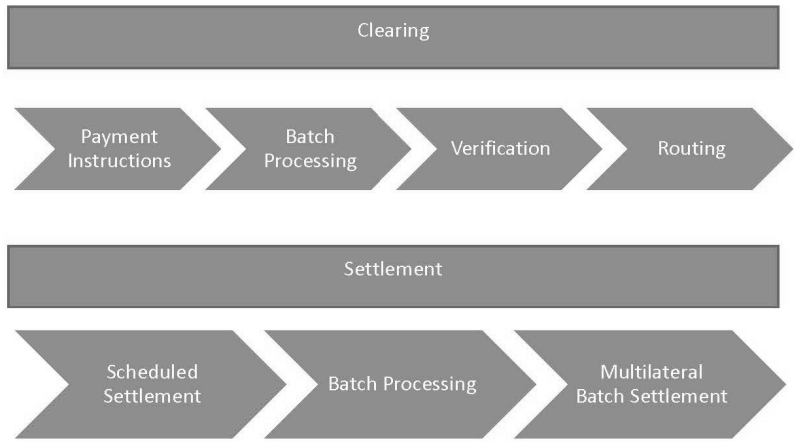
Payment channels are the pathways through which transactions are transmitted. These include physical channels such as bank branches as well as electronic channels like online banking, and mobile banking. Bank

branches provide access to cash and basic banking services. Online banking and mobile banking platforms enable individuals to manage their accounts and initiate transactions remotely.

Clearing and settlement are essential processes within the NPS that ensure the accurate and timely transfer of funds between parties. Clearing is the first step in the process. When a payment is initiated, instructions are sent to the payer's bank. The payer's bank verifies that the payer has sufficient funds. Once verified, the payer's bank sends the payment instructions to the payee's bank. This gives rise to the second step of settlement. Settlement occurs when the funds are transferred from the payer's bank account to the payee's bank account. However, settlement only occurs after the clearing process is completed and the payment instructions are reconciled.

Clearing and settlement occur because of the role the banks play in providing Automated Clearing Houses (ACH). ACH systems are electronic networks that facilitate the transfer of funds between bank accounts, typically for low-value, high-volume transaction stability (Summers, 1994).

Figure 1: Overview of the Clearing and Settlement Process



Source: Author

Therefore, with regard to clearing, the instructions for the payments come to the bank. The instructions are grouped in batches based on their characteristics, such as destination or transaction type for processing by the ACH. Before an instruction is cleared, it is verified as the bank verifies the payer has sufficient funds. Once verified, the payment instructions are

routed through the ACH network to the payee's bank for further processing stability (Summers, 1994).

With regard to settlement, the ACH settles transactions according to predetermined schedules. Based on the operating procedure of the bank providing the ACH services, this may be on a next-day or two-day basis. Within each batch, the total value of incoming payments is offset against the total value of outgoing payments. This netting process is done for liquidity management and improving efficiency. Finally, once the net settlement is calculated, funds are transferred between the banks' settlement accounts to settle the net balance. ACH transactions are settled on a multilateral net basis, meaning that only the net amount owed between banks is transferred, rather than individual transactions stability (Summers, 1994). Figure 1 displays the clearing and settlement process with ACHs.

Thus, ACHs are essential for the national payment system as they act as clearinghouses to process batches of transactions, verify payments, and facilitate net settlement across the local financial landscape.

Alternatively, transactions can also be processed through Real-Time Gross Settlement (RTGS) systems. RTGS is appropriate for clearinghouse services provided for large-value payments such as interbank transfers, securities transactions, and large corporate payments. Unlike ACH transactions, which are processed in batches, RTGS transactions are settled individually and in real-time, providing immediate clearance and settlements of funds. RTGS services are often provided by central banks or designated clearinghouses (Summers, 1994).[2]

Historically central banks held the critical responsibility of ensuring the safety and stability of the payment system. The central bank's three-part mandate includes i) the conduct of monetary policy; ii) oversight of banking and financial markets to ensure their safety and stability; and iii) involvement in the payment system. This was necessary to maintain stability in a country's financial system.

Due to recent advances in technology, as well as the recent COVID-19 pandemic which encouraged the adoption of cashless transactions, digital

[2] Therefore, ACH refers to clearinghouse services provided for low-value high-volume transactions. RTGS refers to clearinghouse services provided for high-value low volume transactions.

payments have been widely adopted. This allows money to flow ever more quickly and efficiently through the payment system.

The following subsection reviews the system for digital payments.

2.2 Electronic Funds Transfers

An electronic funds transfer refers to an instruction from a client to their bank, requesting the transfer of funds from the client's account to the bank account of a designated beneficiary (Mthembu, 2010). EFT has emerged as a dominant means of money transfer due to its convenience, simplicity, and direct means of transferring funds.

An EFT transaction is a simple process involving two parties, namely the sender and the receiver of funds. The sender initiates the transfer, causing the request to travel across digital networks, either via the internet or a payment terminal. The request reaches the sender's bank, which in turn verifies that the sender has sufficient funds before transferring the funds to the receiver's bank. Senders can range from employers to businesses to individuals paying vendors for services. Similarly, recipients can include employees, suppliers of goods, and retailers. Most payments are processed and finalized within a short timeframe, typically within a couple of days.

The popularity of EFT stems from its convenience and rapid delivery. Common EFT methods include direct deposit, direct credit, automatic teller machine (ATM) transactions, point-of-sale transactions, and online banking (CBTT, 2009). Each method offers ease and speed, catering to diverse preferences and needs.

A direct deposit is a convenient method that automatically transfers funds into an account with minimal paperwork. While the process of automatic deposit itself demands little ongoing effort, setting it up initially requires providing bank account details for the recipient, along with any additional required information for setup. Once established, direct deposit offers a seamless and efficient way to make payments regularly (CBTT, 2009).

A direct credit transaction refers to the automated transfer of funds, typically wages or pensions, directly into the bank accounts of individuals. This method offers numerous benefits for both employers and recipients. For employers, direct credit transactions streamline payroll processes, reducing administrative burdens associated with issuing physical checks or manual

payments. Additionally, it ensures timely and accurate payments to employees, enhancing overall efficiency (CBTT, 2009).

ATM transactions take place at electronic kiosks located throughout urban settlements. In these transactions, individuals withdraw cash from their bank accounts by inserting their debit card into the machine, which then transmits information to the bank for processing the request and dispensing money (CBTT, 2009).

In the point-of-sale phase of a transaction, credit cards or debit cards tend to be used for the payment. This payment method involves swiping, dipping, or entering the card details. During this process, account information is electronically received, and the payment withdrawal is approved (Sulaiman & Almunawar, 2022).

Online banking involves individuals using their bank's online banking system to conduct transactions. Through online banking platforms, users can perform various tasks, including transferring funds between accounts, paying bills, and monitoring all of their transactions (CBTT, 2009).

The following subsection reviews the system for international and cross-border payments.

2.3 Cross Cross-Border Payments

When making a payment from one person in a bank in a country to another bank in the same country, the process is typically straightforward. The sender initiates the payment through their bank, providing the necessary details such as the recipient's account number, the amount to be transferred, and any other relevant information. The process of clearance and settlement occurs and ends when there is a direct transfer of funds from the payer's account to the payee's account.

However, when a person wants to make a cross-border payment to another person in another bank in a different country, the process becomes more complex. In this cross-border payment scenario, a correspondent banking relationship is required.

Correspondent banking refers to a relationship established between two banks, typically located in different countries, to facilitate financial transactions on behalf of their respective customers. In this relationship, one bank, known as the "correspondent bank," provides banking services to another bank, known as the "respondent bank."

Correspondent banking requires the respondent bank to open a nostro account in the correspondent bank. When a person from one country attempts to transfer funds to a person in the other country, the respondent bank essentially debts its funds from the Nostro account in the correspondent bank, while the correspondent bank credits the funds from the Nostro account. After the debt and credit transactions of the Nostro account are performed, the correspondent bank then credits the funds to the bank of the payee, who in turn credits the account of the payee.

A key aspect of the cross-border payment system is the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Established in 1973, SWIFT was created to standardize electronic communication systems for payments. Utilizing SWIFT enables banks to employ standardized codes for cross-border transactions, ensuring accuracy in specifying sender and receiver banks. Figure 2 illustrates the cross-border payment system with SWIFT.

As can be seen in Figure 2, the cross-border payment process with SWIFT can involve the transfer of funds through multiple parties to reach the payee. This cross-border payment can often be slow, resulting in clearance and settlement times of 3 to 5 days. This delay can be attributed to several factors, including the need for each intermediary bank to process the funds. The variation in the correspondent banks' processing timelines and operational inefficiencies can contribute to delays in the transmission of funds.

Now that the cross-border payments system is identified, the next sub-section reviews some key considerations of the EFT system, including the need for security, protecting consumers' safety, complying with international financial regulations, and promoting financial inclusion.

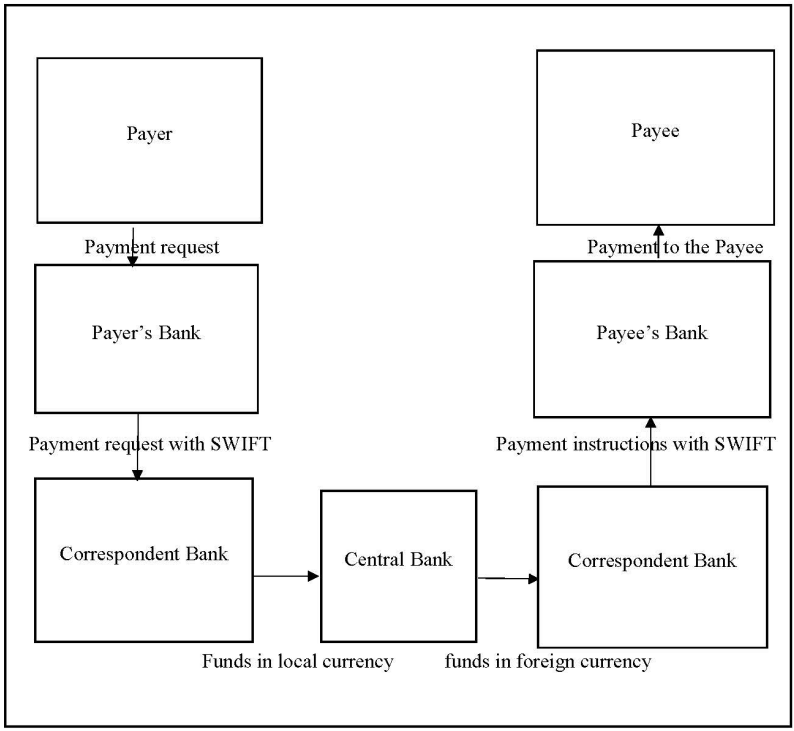
2.4 Key Considerations of EFT Frameworks

The EFT system plays a pivotal role in modern payment systems. Several key considerations are fundamental to ensuring the smooth operation of the EFT system. They are as follows.

2.4.1 Compliance with International Financial Regulators

EFT systems must adhere to a complex web of domestic and international financial regulations to ensure legality, integrity, and stability. Compliance with international financial regulations is essential to mitigate financial crime, prevent illicit activities, and uphold the integrity of the financial system.

Figure 2: SWIFT's Workflow for Cross-Border Payments



Source: Author

2.4.2 Security

Ensuring the security of EFT transactions is important to maintain trust and confidence in the financial system. Robust security measures, such as encryption, multi-factor authentication, and fraud detection systems, are essential to safeguarding sensitive financial data and preventing unauthorized access or cyber-attacks.

2.4.3 Protecting Consumers Safety

Protecting consumers' safety and rights is fundamental to the operation of EFT systems. This includes transparency in transaction fees, timely resolution of disputes, and mechanisms to address unauthorized or fraudulent transactions. Consumer education and awareness campaigns are also vital

to empower individuals with the knowledge and skills to navigate EFT systems.

2.4.4 Financial Inclusion

EFT systems play a crucial role in promoting financial inclusion by expanding access to banking services and enabling participation in the formal financial sector. By offering convenient and affordable digital payment solutions, EFT systems can reach underserved populations, including those in remote areas or with limited access to traditional banking infrastructure. Moreover, initiatives such as mobile banking, digital wallets, and microfinance enable individuals, small businesses, and marginalized communities to engage in economic activities, build savings, and improve livelihoods, thereby fostering financial inclusion.

The next section explores the need to comply the international financial regulations in greater detail.

3. INTERNATIONAL FINANCIAL REGULATION

The regulation of the international finance industry is essential to maintain stability, integrity, and fairness within the global financial system. Regulation serves to establish clear rules and standards for financial institutions while protecting consumers, and the public from exploitation.

3.1 International Financial Regulatory Institutions

The international finance environment is regulated by the rules established by several bodies, namely the Financial Action Task Force (FATF), the Financial Stability Board (FSB), the US Foreign Account Tax Compliance Act (FATCA), the Organization for Economic Cooperation and Development's (OECD's) Common Reporting Standards (CRS), and the Action Plan on Base Erosion and Profit Shifting (BEPS), and the United Kingdom's (UK's) Public Registry of Beneficial Ownership (PRBO). The corresponding regulatory institutions are reviewed in the following subsections.

3.2 The Financial Action Task Force

Established in 1989 at the behest of the G7, the Financial Action Task Force is an intergovernmental organization tasked with formulating policies aimed at combating money laundering, terrorist financing, and threats to the global financial system. The FATF Recommendations outline a comprehensive set of measures that member countries are encouraged to adopt to address money laundering and terrorism financing, as well as related illicit activities (FATF, 2012).

Notably, countries have varying legal, administrative, and financial frameworks, making it challenging for them to uniformly address threats such as money laundering and terrorist financing. Despite these differences, the FATF Recommendations serve as a guideline for countries to strive towards implementing appropriate measures. However, certain measures are obligatory for countries to adopt to maintain banking and financial relationships with FATF member nations. These include:

- Implementing measures to assess risks associated with money laundering and terrorist financing.
- Formulating policies to prevent money laundering and terrorist financing.
- Enforcing preventive measures within the financial sector and other designated sectors.
- Granting national security authorities, the power to combat money laundering and terrorist financing.
- Enhancing transparency by disclosing beneficial ownership information of legal entities and arrangements.
- Facilitating international cooperation in combating financial crimes (FATF, 2012).

3.3 The Financial Stability Board

The Financial Stability Board is an international organization tasked with overseeing and providing recommendations to safeguard the integrity of the global financial system. It collaborates closely with national financial authorities and international standard-setting bodies to develop robust regulatory policies for the financial sector. Specifically, the FSB was established to:

- Assess vulnerabilities impacting the global financial system.
- Identify and evaluate regulatory and supervisory actions necessary to address these vulnerabilities.
- Promote the exchange of information among authorities responsible for maintaining financial stability.
- Monitor market developments and advocate for regulatory policies based on best practices.
- Enhance contingency planning for managing cross-border crises, particularly involving systemically important firms.
- Conduct joint exercises with the International Monetary Fund (IMF) to assess potential risks early on.
- Perform strategic reviews of international standard-setting bodies and ensure their focus aligns with priorities and addresses any gaps.
- Assist member jurisdictions in implementing agreed-upon commitments, standards, and policy recommendations (Gadinis, 2013).

3.4 The Foreign Account Tax Compliance Act

Introduced in 2010 by the United States (US) authorities, the Foreign Account Tax Compliance Act mandates all non-US financial institutions to disclose the foreign assets held by their US account holders to the US Department of the Treasury. Non-US banks are obligated to adhere to FATCA regulations, facing a 30% withholding penalty on all US transactions in case of non-compliance.

The primary objective of FACTCA was to identify US citizens and residents with financial assets overseas and assess the extent of these holdings. Currently, FATCA is utilized to uncover assets rather than income and does not include provisions for imposing taxes directly. However, US residents and citizens, irrespective of dual nationality, are mandated to annually self-report their non-US assets to the Financial Crimes Enforcement Network (FinCEN) and the Internal Revenue Service (IRS). FATCA facilitates the identification of individuals who have failed to self-report or file any overdue Report of Foreign Bank and Financial Accounts (FBAR).[3]

3.5 The Common Reporting Standards

The Organization for Economic Co-operation and Development (OECD) introduced the Common Reporting Standard (CRS) in 2014. This framework facilitates the automatic exchange of tax and financial data among jurisdictions. Initially, forty-seven countries[4] provisionally endorsed the Standard for Automatic Exchange of Financial Account Information, commonly known as the CRS, enabling jurisdictions to automatically share information regarding residents' assets and incomes. The primary aim of the CRS is to address tax evasion globally, making it akin to the OECD's counterpart to FATCA (PWC, 2015).

---

[3] All US residents or citizens who possessed a financial interest in or authority to sign over at least one financial account situated outside of the United States, and if the combined value of all foreign financial accounts surpassed US$10,000 at any point during the calendar year in question, must submit an FBAR. Individuals who failed to file an FBAR on time are obligated to submit a delinquent FBAR (IRS, 2024).

[4] The CRS was agreed upon by all thirty-four OECD countries, along with Argentina, Brazil, China, Colombia, Costa Rica, India, Indonesia, Latvia, Lithuania, Malaysia, Saudi Arabia, Singapore, and South Africa.

Prior to the implementation of the CRS, the exchange of financial information between countries was conducted on a request basis, with authorities deciding the extent of information to be exchanged. With the introduction of the Automatic Exchange of Information (AEoI) through the CRS, tax authorities can now automatically share financial information in agreed-upon formats at scheduled intervals through established channels. The CRS broadens the scope of information exchange (PWC, 2015).

It is important to highlight that FATCA functions through bilateral agreements between the US and individual countries, whereas the CRS operates under a Competent Authority Agreement (CAA) framework. The CRS relies on two types of CAAs: bilateral and multilateral. A bilateral CAA entails an agreement for information exchange solely between the tax authorities of two jurisdictions, while a multilateral CAA (MCAA) involves multiple jurisdictions as signatories, with each jurisdiction exchanging information with all other signatories to the MCAA (PWC, 2015).

3.6 Action Plan on Base Erosion and Profit Shifting

The consequence of transfer pricing is a decrease in tax payments to governments. This poses a challenge for countries as the foregone tax revenue could have supported various national development goals. Additionally, this places a heavier tax burden on entities that diligently fulfill their tax obligations. Acknowledging the potential for multinational corporations to exploit tax disparities between nations, the OECD and G20 established the Inclusive Framework on Base Erosion and Profit Shifting to address this issue. With 108 members, this framework focuses on combating tax avoidance by ensuring the implementation of measures outlined in the BEPS Project, which targets aggressive tax evasion practices among multinational companies. The BEPS measures center around four “minimum standards”, namely: addressing harmful tax practices; preventing treaty abuse; enhancing country-by-country reporting; and improving dispute resolution mechanisms (OECD, 2018).

The OECD has created the Action Plan on Base Erosion and Profit Shifting to address loopholes that enable multinational corporations to exploit tax differences between countries and minimize their tax obligations. This initiative aims to equip countries with both domestic and international tools to ensure that taxation aligns more closely with economic activity. The Action Plan involves:

i. Identifying necessary actions to combat BEPS;
ii. Establishing timelines for implementing these actions; and
iii. Determining the resources required to administer these measures (OECD, 2015).

The OECD also has the BEPS Package, which is comprised of fifteen actions that are supposed to equip governments with further tools to tackle base erosion and profit shifting (Peeters & Vanneste, 2020). Additionally, the OECD also has the Global Forum on Transparency and Exchange of Information for Tax Purposes as a framework to combat tax evasion.

3.7 Public Registry of Beneficial Ownership

In June 2016, the United Kingdom became the inaugural G20 nation to implement a public register disclosing the beneficial owners of companies. This register was introduced as a measure to combat corruption and tax evasion, providing transparency regarding the ownership of UK-based companies. A similar initiative is anticipated within the European Union (EU), as Article 30 of the 4th EU Anti-Money Laundering Directive (4AMLD) mandates all EU Member States to enact legislation that publicly discloses beneficial ownership information for corporate and legal entities (HM Government, 2017).

3.8 Anti-Money Laundering / Counter-Financing of Terrorism Measures Required by Banks

As a consequence of the financial regulation set by the international authorities, banks must implement an anti-money laundering (AML) compliance program to address 4 strategic areas.

1. Know-Your-Customer.

The first requirement is called “Know-Your-Customer”. This is where banks gather customer information and validate its accuracy. This measure aims to mitigate the risk of identity fraud by ensuring that a customer's digital identity aligns with their real-world identity. Verification procedures may include requesting two forms of identification, proof of address (such as utility bills), and conducting facial recognition verification.

2. Customer due diligence (CDD).

The second requirement is called “Customer-due-diligence”. This involves the collection and assessment of a customer's information to ascertain the risk of potential money laundering and financing of terrorist activities. This process includes cross-referencing a customer’s details with international watchlists, which encompass politically exposed persons, government records, and lists of sanctioned entities, to ensure compliance with regulations and mitigate financial crime risks.

3. Customer and transaction screening.

The third requirement is for customer and transaction screening. This is where banks are mandated to monitor all transactions conducted by their customers to verify that they are not involved in any money laundering activities.

4. Suspicious activity reporting.

The fourth requirement pertains to suspicious activity reporting. In cases where there is suspicion of money laundering or terrorism financing, banks are obligated to report such instances to their national or regional financial regulatory authority.

The interconnected nature of global financial systems means that breaches in the security of financial institutions can compromise the customer information collected. Additionally, cyber threats can undermine efforts to address money laundering and the financing of terrorism.

3.9 Payment Card Industry Security Standards

The Payment Card Industry Security Standards Council (PCI SSC) was established with the primary objective of enhancing data security for payment cards and minimizing the occurrence of data breaches and payment cardholder data fraud. By setting industry-wide standards, the PCI SSC seeks to foster a secure environment for payment card transactions, thereby bolstering consumer confidence in the safety and reliability of electronic payments. The PCI Data Security Standard (PCI DSS) forms the cornerstone of the PCI SSC’s efforts to fortify payment card security. Comprising 12 fundamental requirements, the PCI DSS delineates comprehensive guidelines for safeguarding cardholder data and securing payment card transactions (Surya et al., 2023). They are outlined in Table 1.

Table 1: PCI Data Security Standards

Name of Standard	Details	
Build and maintain a secure network and systems	1	Establish and maintain a firewall configuration to safeguard cardholder data.
	2	Avoid using the default settings provided by vendors for system passwords and other security parameters.
Protect Cardholder Data	3	Safeguard stored cardholder data.
	4	Cardholder data that are transmitted across public networks should be encrypted.
Maintain a Vulnerability Management Program	5	Update anti-virus software regularly, and protect the systems from viruses and other malware.
	6	Make the systems secure and maintain the security.
Implement Strong Access Control Measures	7	Limit access to cardholder data to individuals with a business need to know.
	8	Authenticate and authorize access to system components.
	9	Limit people from physically accessing cardholder data
Maintain an information security policy	10	The access to network resources and cardholder data should be monitored and tracked.
	11	Regularly test systems to ensure there is good security.
	12	Establish a comprehensive policy addressing information security for all personnel.

Source: Surya et al. (2023)

The distribution of liability for payment card fraud tends to fall on the issuers, and merchants rather than the cardholders. This distribution of liability is designed to incentivize these stakeholders to implement and maintain robust security measures to protect cardholder data and prevent fraudulent activities. However, this arrangement can lead to disputes, particularly regarding the allocation of costs associated with compliance with the PCI DSS requirements. Merchant groups, in particular, have raised concerns about the burden of compliance costs, arguing that PCI DSS standards are often rigid and costly to implement, especially for small and

medium-sized businesses. Additionally, there have been criticisms that PCI DSS standards primarily serve the interests of card networks and issuers, rather than addressing the broader security needs of the payment card ecosystem (Surya et al., 2023).

The enforcement of PCI DSS compliance is primarily driven by card networks, which require participants to adhere to these standards through network agreements. Non-compliance can result in fines, penalties, and liability shifting, further incentivizing stakeholders to maintain compliance. However, this enforcement mechanism has also been criticized, with some stakeholders arguing that it places undue financial and operational burdens on merchants and processors. Moreover, there have been concerns about the effectiveness of PCI DSS standards in adequately addressing evolving cybersecurity threats and vulnerabilities in the payment card industry. As such, there is ongoing debate within the industry regarding the balance between security requirements, compliance costs, and the overall effectiveness of PCI DSS standards (Surya et al., 2023).

The next section delves deeper into the cybersecurity risks and mitigation strategies associated with electronic funds transfer.

4. CYBERSECURITY

Cybersecurity encompasses processes aimed at defending computers, servers, networks, and digital data from unauthorized access. It involves implementing measures to safeguard against a wide range of threats, including malware, phishing, ransomware, and hacking attempts. This field applies to various sectors, including telecommunications, finance, and any other sector with sensitive data. With regard to the finance sector, the increased reliance on technology for automation has made the sector more vulnerable to cyber threats. Moreover, financial institutions hold valuable client data and funds, making them lucrative targets for cybercriminals. Therefore, cybersecurity is a paramount concern for the financial sector, to protect from data breaches, and the unauthorized access of funds (Baur-Yazbeck et al., 2019). The following subsections consider the issues regarding cybersecurity in the electronic funds transfer industry.

4.1 Understanding Cybersecurity Risks

Consumers can be targeted with cyber fraud through various forms, such as deceptive SMS, emails, or phone calls urging recipients to send money or disclose sensitive personal information like PINs. This information is then exploited for account takeover or identity theft purposes. Alternatively, the fraud may manifest as unauthorized transactions conducted from the victims' accounts without their consent. Moreover, cyber incidents can lead to system downtime, preventing customers from accessing their funds, and thereby exacerbating the impact of the fraud.

Fraudsters commonly exploit vulnerabilities within the EFT system, encompassing EFT providers, payment and settlement systems, point-of-sale networks, regulators, and customers, to gain access, disclose, or exploit critical information for monetary gain. Predominant cybercrime-related threats include data breaches, customer identity theft, and fraudulent money transfers.

Baur-Yazbeck et al. (2019) identifies four types of cyberattacks that frequently affect EFT. They include the following.

1. The first type of attack is phishing. This involves a fraudster manipulating either a customer or an employee of a service provider, persuading them to divulge confidential information or grant access to internal systems and databases. This manipulation often occurs through several methods such as fraudulent phone calls, text messages (SMS), or emails. The aim is to obtain personally identifiable information such as credit card numbers, PINs, and account login credentials. Subsequently, this acquired information is exploited to perpetrate identity theft, gain control over accounts, and access customer funds (Baur-Yazbeck et al., 2019).
2. The second type of attack is fraud. This includes fraudulent activities committed by individuals with privileged access or insider knowledge within an organization. This can include employees, contractors, or partners who misuse their authorized access for malicious purposes, such as theft, fraud, or sabotage. One type of fraud is card fraud where a merchant's point-of-sale system is hacked, the card information is stolen, and the thieves produce counterfeit cards with the stolen data and make unauthorized purchases (Scanio & Glasgow, 2015).
3. The third type of attack is malware, ransomware and denial of service. These attacks hinder provider staff, customers, and/or third-party systems from accessing an ETF platform and its services. Additionally, they can serve as a means to conceal a data breach (Baur-Yazbeck et al., 2019). These types of cyberattacks can also be backdoor attacks whereby a hacker gains unauthorized access by circumventing standard authentication mechanisms. These attacks may occur discreetly in the background and remain concealed from users, posing challenges for detection and removal (Surya et al., 2023).
4. The fourth type of attack is a scam. Advance fee scams and transfer reversal requests are among the most prevalent EFT scams. In an advance fee scam, individuals are deceived into sending money to purportedly participate in a false lottery or to claim a counterfeit reward or gift. Conversely, in a reversal request, customers are asked to refund an erroneous deposit that has been transferred into their account (Baur-Yazbeck et al., 2019).

Based on the aforementioned risks, cyber and data security should prioritize achieving two critical goals. The first goal is the safeguarding of data, particularly sensitive and personally identifiable information (PII) from unauthorized access. Security measures, including encryption, access

controls, and regular monitoring, are essential to prevent unauthorized access.

The second goal is the protection of financial systems from cyberattacks. Implementing robust cybersecurity measures, including intrusion detection systems, network firewalls, and regular security audits, is essential to mitigate the risks posed by cyber threats and ensure the reliability and efficiency of the EFT system (Baur-Yazbeck et al., 2019; Khan & Malaika, 2021).

In many developing countries, the fight against cybercrime faces significant challenges due to inadequate legislation, insufficient punishments, and a shortage of legal expertise necessary for prosecuting cybercrimes. Moreover, procedural hurdles such as jurisdictional issues, maintaining evidentiary standards, and explaining complex digital crimes to juries further impede effective prosecution. As a result, cybercriminals often operate with impunity (Baur-Yazbeck et al., 2019; Khan & Malaika, 2021). To address these challenges, a comprehensive approach is required, focusing on the development of regulatory frameworks, industry guidance, and supervisory processes to enhance cybersecurity measures. The next subsection explores the approaches adopted by several countries to address cybersecurity risks to the EFT industry.

4.2 Country Approaches for Addressing Cybersecurity Risks

In many developing countries, government-led cybersecurity efforts often prioritize serving public agencies and critical infrastructure. Government agencies may have national support structures such as computer emergency response teams (CERTs) or national computer security incident response teams (CSIRTs). Unfortunately, these entities frequently lack the capacity and resources to effectively address the evolving cyber threat landscape. Moreover, specialized CERTs focusing on financial sector threats are rare, and those that do exist often offer limited services, lack 24/7 availability, and have minimal resources for emergency response. Critical service gaps often persist in developing countries, including the absence of security operations centers, industry-wide threat information-sharing mechanisms, policy advisory services, sector-specific guidance, and educational programs for businesses and individuals (Baur-Yazbeck et al., 2019).

Nevertheless, several countries experiences can stand as commendable practices to be replicated. For instance, Ghana’s National Information