JGB 3614

The Cybercrime, Anti-Money Laundering, and Data Protection Issues Surrounding Unverified E-Wallet Accounts

Atty. Jan Raphael Salud & Hannah Louise Lee

De La Salle University, Manila

jan.salud@dlsu.edu.ph & hannah_louise_lee@dlsu.edu.ph

Abstract

The shift from a policy-based approach to a risk-based approach to anti-money laundering regulations in the Philippines enabled Electronic Money Issuers (EMIs) to adopt a Reduced Due Diligence Procedure for accounts used purely for digital or electronic payments. The resulting tiered system of identification and validation of users dispenses with the identification and verification process for specific accounts, which, unfortunately, contributed to the proliferation of cybercrime. In this paper, the EMI's tiered system and creation of unverified e-wallet accounts will be examined in the context of the Anti-Money Laundering Act of 2001, among other related laws on e-money transactions. This paper suggests that e-wallet users have general but not individual consumer rights due to the lack of concrete regulations on the nuances of financial technology; in fact, redress for infringement of rights is limited to contractual relationships of users with EMIs. Lastly, this paper discusses the possible breach of the Data Privacy Act of 2012, should the aggrieved consumer maintain suit involving a crime facilitated through an EMI platform. As Financial Technology continues to revolutionize financial services, addressing the conceivable perils identified herein will eliminate legal

impediments but will also incite further advancements accessible, especially by the unbanked and underbanked.

Keywords: *Electronic Money, Anti-Money Laundering, Data Privacy, Consumer Rights*

Introduction

Financial Technology (FinTech) has been rising as it continuously develops alongside new technological advancements (Arner et al., 2016). It has caught the attention of key players in the Sustainable Agenda of the United Nations (Agenda for Sustainable Development, 2030). It has been incorporated into Goal 8 – promoting sustained, inclusive, and sustainable economic growth, full employment, and decent work for all (United Nations, 2016). Under the UN Task Force on Digital Financing of Sustainable Development Goals' action plan, FinTech companies are called to innovate products and services that adhere to consumer demand to channel finance to sustainable development (United Nations, 2020). In Southeast Asia, the impact of fintech has been evident in accommodating the unbanked (Soriano et al., 2019).

In the thick of the Novel Coronavirus 2019 (COVID-19) pandemic, Filipinos turned to online banking, electronic wallet (e-wallets), and digital payment systems to facilitate commercial transactions. The need for social distancing pushed the cash-centric and face-to-face shopping culture towards a more digital one. In the same way, different companies such as telcos, banks, and fintech start-ups have rolled out e-wallets for unbanked populations. Significant players include PayMaya and GCash. The Bangko Sentral ng Pilipinas (BSP) — the Philippine Central Bank — also launched PESONet, a new electronic funds transfer service that enables customers of participating banks, e-money issuers, or mobile money operators to transfer

funds in Philippine Peso currency to another customer of other participating banks, e-money issuers, or mobile money operators in the Philippines (Country Commercial Guide, 2021).

Covid-19 Lockdowns and restrictions in the Philippines simulated the increased demand for cashless payments and boosted financial inclusion (Beltran, 2022). BSP anticipates that by 2023, 50% of all retail transactions will be digital, and 70% of Filipino adults will be financially included (Quintero et al., 2022). Mobile wallets and e-money have been identified as the primary driver of FinTech growth in the Philippines (Santiago, 2021). Its consistent growth adversely affects traditional banking, especially since banks need to be faster in developing digital services (FinTech News Philippines, 2021). E-money has been defined as an acceptable mode of payment, the monetary value of which is electronically stored and may be claimed from its issuer and withdrawn as cash or cash equivalent (Manual of Regulations for Banks, §702). The growth of e-money has been consistent at 8% since 2014 (Santiago, 2021); such a trend is expected to advance steadily due to the country's digitalization efforts and favorable regulatory environment (Quientero et al., 2022). Despite the positive outlook on e-money, unfortunately, the increase in the use of online payment systems also contributed to the proliferation of cybercrimes that take advantage of the nuances of financial technology (FinTech).

In October 2020, the Philippine National Police Anti-Cybercrime Group (PNP-ACG) revealed that 869 online scams were recorded from March to September 2020 — a 37.28 % increase compared to the previous year (Tupas, 2021). Within the same period, the Anti-Money Laundering Council (AMLC) observed a 57% increase in suspicious transaction reports received from January to August 2020 (Ditas, 2020). These cybercrimes involve phishing, smishing, vishing, and other online fraud schemes, which are expected to increase further as more transactions shift online (Balinbin, 2021).

Tupas (2020) reports that unscrupulous individuals have been using Facebook and other social media platforms to sell items that never arrive or are different from the original item advertised. For instance, a 24-year-old in San Pedro City, Laguna, Philippines, lost P17,500.00 after purchasing an iPhone 11 advertised through the social media platform Instagram. The suspect, who identified herself to the victim as Yvonne Villasica, could no longer be contacted after receiving payment through GCash. Another victim recounts having purchased pet apparel from a certain Marilyn De La Cruz, a person she met on Facebook (M.Pat, 2021). After asking Marian to transfer P9,200.00 to her GCash Account, Marilyn quickly deactivated her Facebook account and kept herself out of reach. Esquire (n.a., 2020) also accounts for individuals posing as typhoon victims and advertising their GCash accounts to solicit donations online. Due to the ease of sending money through e-wallets, bogus sellers or donees could dupe people into sending them money instantly. The foregoing incidents have one thing in common — the perpetrators facilitated their schemes through unverified e-wallet accounts.

In any case, under present regulations, Electronic Money Issuers (EMIs) could readily refuse to render meaningful assistance to the investigation of criminals who utilized their platforms by arguing that: (1) they have complied with the minimum reportorial requirements under the Anti-Money Laundering Act of 2001 (AMLA), as amended, and that the same is the extent of their obligation; and (2) their obligations under the Data Privacy Act of 2012 (DPA) prevent them from disclosing the information of the suspected criminal, even though the said accounts were unverified.

During the Senate Committee on Public Order hearing, Sen. Tolentino expressed his concern for the inadequate procedures carried out by EMIs in identifying its subscribers. The BSP and Anti-Money Laundering Council (AMLC) shared the same concerns and thus directed

financial services providers to revamp their cybersecurity systems to counter unlawful access and compromise of accounts effectively. Through FinTech Alliance. P.H. and eMoney Association, the private sector, also launched an advocacy campaign on the responsible use of digital payment platforms ("E-wallets and illegal activities," 2022). Regulators and interested agencies remain looking for illegal activities that may be facilitated through e-wallets. However, e-wallets remain vulnerable due to their very nature and nuances to technology. Specific beneficial characteristics of the technology also pose risks; among such risks associated with e-wallets are lack of supervision, speed of transaction, insufficient user identity verification procedures (anonymity), and concealment of transactions ("E-wallet and Anti-Money Laundering in the Philippines," 2022).

Framework

This paper discusses FinTech ecosystems and platforms in general, focusing on e-wallets and Electronic Money Issuers (EMIs). It excludes virtual currencies (V.C.) and virtual asset service providers (VASPs) from its scope. While V.C.s and VASPs are components of the broader FinTech industry, this paper focuses on e-money, a FinTech product generally accessible to the most transacting public. More importantly, Virtual Assets are not issued nor guaranteed by any jurisdiction and do not have legal tender status. In contrast, e-money in the Philippines is backed up by a 1:1 ratio of fiat money.

Furthermore, this paper discusses the legal framework surrounding e-wallets and EMIs in the context of consumer rights protection. As a FinTech actor operating a money service business, EMIs are covered by the AMLA, which explicitly prohibits anonymous accounts under fictitious names. Unfortunately, the reduced due diligence (RDD) measures, which most EMIs adapt to the government's risk-based approach in money laundering, effectively dispense with

identification and verification requirements. In effect, users are exposed to inherent risks and nuances of FinTech without sufficient legal safeguards and adequate remedial measures in case the said platforms are used to facilitate fraudulent transactions. Lastly, this paper also reveals that the right of the victims to compel EMIs to disclose information, which could lead to the identification and successful prosecution of e-wallet users, remains convoluted.

Methodology

This paper is primarily based on the Master of Laws thesis of Atty. Jan Raphael Salud in the Ateneo de Manila University School of Law. The paper employed a qualitative and doctrinal research methodology and looked into domestic law, soft international law, and commentaries relevant to Anti-Money Laundering and Data Privacy; It also looked into the Electronic Commerce Act, the various issuances of the BSP, including and especially the Manual of Regulations for Non-Bank Financial Intuitions (MORNBFI). The end-user agreements of some EMIs listed and supervised by the BSP were examined and used in constructing the matrix on the tiered verification schemes. Only information pertinent to EMIs with at least 1,000,000 customers and 10,000 partner merchants was reviewed for practicality. This research's EMIs and account verification processes are accurate only as of May 2021.

Discussion of Results

The Anti-Money Laundering Act of 2001 (AMLA) criminalized acts involving transactions of proceeds of unlawful activities, which were made to appear to have originated from legitimate sources. To prevent the commission and aid in the prosecution of money laundering, Section 9 of the said law explicitly provides that “the provisions of existing laws to the contrary notwithstanding, anonymous accounts, accounts under fictitious names, and all other

similar accounts shall be prohibited" (Anti-Money Laundering Act, 2001). Although AMLA underwent several amendments, Section 9 remains intact to this day.

The blocklisting of the Philippines prompted the passage of the Anti-Money Laundering Act of 2001 by the Financial Action Taskforce (FATF) (Cantorias, 2021), an international independent and inter-governmental body that develops and promotes policies to protect the global financial system against money laundering (ML), terrorist financing (T.F.), and the financing of proliferation of weapons of mass destruction. FATF Recommendations are recognized as the global anti-money laundering and counter-terrorist financing standard (Financial Action Task Force, 2022).

On March 8, 2002, the Anti-Money Laundering Council issued its first implementing rules and regulations (IRR). In its embryonic state, the 2002 IRR adopted the following rules on customer identification —

RULE 9.1.a. Customer Identification. — Covered institutions shall establish and record the true identity of their clients based on official documents. They shall maintain a system of verifying the true identity of their clients and, in the case of corporate clients, require a system of verifying their legal existence and organizational structure, as well as the authority and identification of all persons purporting to act on their behalf. Covered institutions shall establish appropriate systems and methods based on internationally compliant standards and adequate internal controls for verifying and recording their customers' accurate and complete identity (Rules and Regulations Implementing the Anti-Money Laundering Act of 2001, 2002)."

Under the 2002 IRR, covered institutions "shall require customers to produce original documents of identity issued by an official authority, bearing a photograph of the customer. Examples of such documents are identity cards and passports" (Rules and Regulations Implementing the Anti-

Money Laundering Act of 2001, 2002). This IRR portion, commonly known as Know-Your-Customer or KYC, was substantially retained by the AMLC in its August 6, 2003, IRR (Rules and Regulations Implementing the Anti-Money Laundering Act of 2001, 2003). The 2002 and 2003 IRRs thus adopted a policy-based approach wherein the AMLC required all covered institutions to implement a uniform customer identification system regardless of the transaction involved (Rules and Regulations Implementing the Anti-Money Laundering Act of 2001, 2002).

In 2012, the FATF introduced the risk-based approach to anti-money laundering regulation. The FATF recommends,

As a basic principle, financial institutions and DNFBPs (Designated Non-Financial Businesses and Professions) should be required to take steps to identify and assess their money laundering/financing threat risks for customers, countries or geographic areas, and products/services/transactions/delivery channels. Additionally, they should have policies, controls, and procedures in place to effectively manage and mitigate their risks, which should be approved by senior management and be consistent with national requirements and guidance (Jeans, 2016).

Taking its cue from the FATF, the AMLC revised the AMLA IRR in 2012 and adopted the risk-based approach. Under Rule 9.a.9 of the 2012 IRR: "[a] covered institution shall develop clear, written and graduated customer acceptance policies and procedures including a set of criteria for customers that are likely to pose a low, normal or high risk to their operations as well as the standards in applying reduced, average and enhanced due diligence including a set of conditions for the denial of account opening" (Revised Rules and Regulations Implementing the Anti-Money Laundering Act of 2001, 2012). This led to the introduction of various levels of customer due diligence, to wit:

Enhanced Due Diligence (EDD) “refers to the enhanced level of scrutiny intended to provide a more comprehensive understanding of the risks associated with the client, as well as confirmation of factual information provided by the client, to mitigate risks presented;." Average Due Diligence (ADD) “refers to the normal level of customer due diligence that is appropriate in cases where there is a medium risk of money laundering or terrorism financing;” and Reduced Due Diligence (RDD) "refers to the lowest level of customer due diligence that is appropriate in cases where there is a low risk of money laundering or terrorism financing” (Revised Rules and Regulations Implementing the Anti-Money Laundering Act of 2001, 2003). Section 11.2 of the 2012 IRR also provided that:

11.2. In strictly limited circumstances and where there is a proven low risk of ML/TF. The [Supervising Authorities (S.A.s)] may issue guidelines allowing certain exemptions on CDD measures, taking into account the nature of the product, type of business, and the risks involved, Provided that ML/TF risks are effectively managed (Revised Rules and Regulations Implementing the Anti-Money Laundering Act of 2001, 2018).

Electronic money (e-money) regulation dates back to 2009 with BSP's issuance of Circular No. 649. The administrative circular set guidelines on the issuance of e-money and the operations of Electronic Money Issuers (EMIs). BSP Circular No. 649 was later incorporated in the Manual of Regulation for Non-Bank Financial Institutions (MORNBFI) as Sections 4642N to 4642N.7 (Bangko Sentral ng Pilipinas, 2017).

In 2018, BSP issued Circular No. 1022 (Bangko Sentral ng Pilipinas, 2018). It amended pertinent provisions of the Manual of Regulations for Banks (MORB) and the MORNBFI. Specifically, it outlined the risk-based approach procedures to be observed by banks and Non-Bank Financial Institutions (NBFIs), including EMIs. Specifically, for RDD, it provided that:

"d. Reduced due diligence. Where lower risks of ML/TF have been identified through an adequate analysis of risk by the covered person and based on the results of the institutional risk assessment, reduced due diligence procedures may be applied commensurate with the lower risk factors. The reduced due diligence procedures shall not be applied in cases of suspicion of higher ML/TF risk scenarios.

“Whenever reduced due diligence is applied as provided in this part of the covered person's customer acceptance policy, the following rules shall apply:

“(1) For individual customers, a covered person may open an account/establish relationship under the true and full name of the account owner/s or customers upon presentation of an acceptable identification card (lD) or official document as defined in this part or other reliable, independent source documents, data or information: Provided, That, for accounts used purely for digital or electronic payments, the covered person may define appropriate reduced due diligence procedures provided that ML/TF risks are effectively managed.

“Verifying the customer's identity, beneficial owner, or authorized signatory can be made after establishing the business relationship” (Bangko Sentral ng Pilipinas, 2018).

The above regulations from the AMLC and BSP enabled EMIs to adopt a tiered system of identification and validation of users. Under this system, users can establish business relationships with EMIs without undergoing full customer identification and verification processes so long as their access to e-wallet services is limited. As of May 2021, the following matrix demonstrates the tiered-verification schemes adopted by some significant EMIs:

EMI	PLATFORM	TIERED VERIFICATION	ACCOUNT LIMITATIONS
AirPay Technologies Philippines, Inc.	ShoppeePay	Yes	Once an Account is set up, you can directly transact. However, you can store a maximum of PHP 50,000 in the account with further verification. By setting up an Account, you confirm that you have provided us with your consent to use your personal information stored by the relevant 3P Merchant for verification if required, including, but not limited to, when your account mobile-activated phone has been lost, stolen or deactivated. To be a verified user, you must submit a picture of you and your identity card, address, birth date and birthplace, and identity card number. Once verified, you can store a maximum of PHP100,000 in the account. The maximum limit of monthly incoming funds for verified and unverified Accounts is PHP50,000 and PHP 100,000, respectively. By registering for an Account, you confirm that (a) you have provided us with your consent to use your personal information for the provision of Services; and (b) you will pay or allow us to deduct from your account all fees associated with the use of the Services (ShopeePay, 2021).
DCPay Philippines, Inc	Coins.ph	Yes	Level 1: Once you sign up and confirm your email address or mobile number, your account is at Level 1 by default. Your limit is 2,000 PHP per day for cash-ins, and you cannot create cash-out orders. Level 2: Level 2 accounts have a cash-in and cash-out limit of 50,000 PHP per day and 400,000 PHP per year. To reach Level 2, you must complete I.D. and selfie verification.

EMI	PLATFORM	TIERED VERIFICATION	ACCOUNT LIMITATIONS
			To complete the selfie verification, click here and take a photo of yourself while holding up your I.D. This information is necessary to provide you with a secure and personalized experience, prevent fraud from occurring on our platform, and comply with local regulations. We take your privacy very seriously. Level 3: Level 3 accounts have a cash-in and cash-out limit of 400,000 PHP per day. To reach Level 3, you must have your account address verified. Level 4: Level 4 accounts provide custom limits for customers who require transaction limits beyond those offered in Level 3 (Coins.ph, 2022).
Gpay Network P.H., Inc	GrabPay	No (Grab, 2019)	
G-Xchange, Inc	GCash	Yes	Basic User (Level 1/Non-verified) - you have only just registered to GCash and can access essential GCash services, but you have the option to be verified further. Basic Users only have access to the following: Cash-In (Over-the-Counter channels only) Pay Bills Buy Load Borrow Load Book Movies Fully Verified (Level 3) - you have completed the verification process and submitted a valid I.D. Enjoy the following features as a Fully Verified GCash customer:

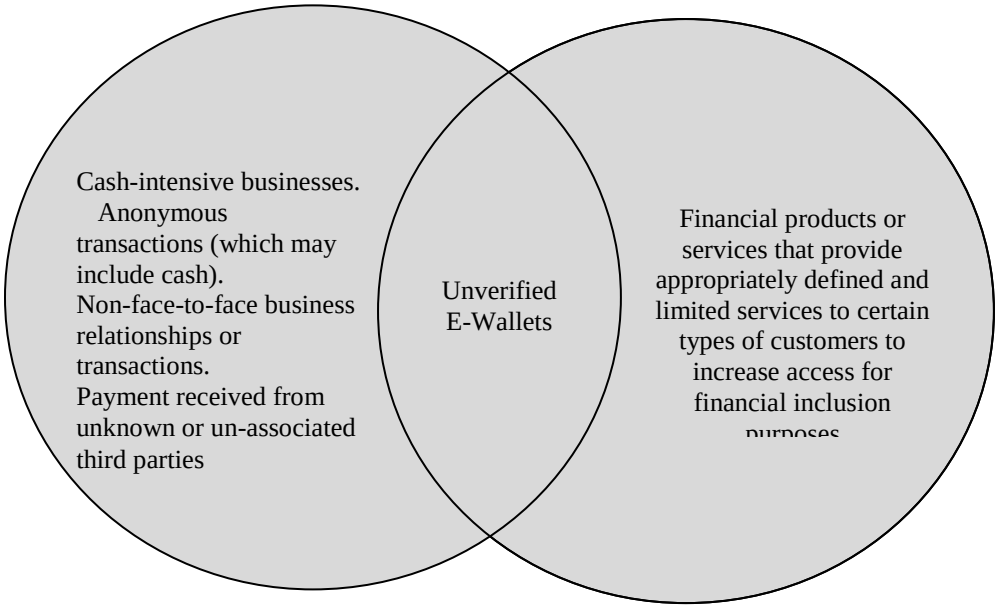
EMI	PLATFORM	TIERED VERIFICATION	ACCOUNT LIMITATIONS
			Increased wallet limit to Php 100,000 Full access to all GCash services ATM withdrawals up to Php 40,000 daily and Buy Load transactions (to Globe and other networks) up to Php 20,000 daily (GCash, 2021).
Paymaya Philippines, Inc.	PayMaya	Yes	If your account is not yet upgraded: You cannot send money using your PayMaya app You cannot withdraw money at ATMs using your PayMaya card You can only add money of up to PHP 50,000 per month You can only spend up to PHP 50,000 per month Your PayMaya wallet can only maintain a maximum balance of PHP 50,000 per month If your account is already upgraded: You can send money to other PayMaya users using your PayMaya app You can transfer money to your bank accounts You can activate the free virtual card that you can use for online transactions You can withdraw money at ATMs using your physical PayMaya card You can add money of up to PHP 100,000 per month You can spend up to PHP 100,000 per month Your PayMaya wallet can maintain a maximum balance of PHP 100,000 per month (PayMaya, 2022)
TrueMoney Philippines Inc.	TrueMoney	No (TrueMoney, 2021)	N/A

Considering the foregoing, it is important to examine whether unverified e-wallet accounts covered by reduced due diligence measures are in accord with the FAFT regulations. According to FATF Recommendations, cash-intensive businesses and products or services which involve transactions that are anonymous, non-face-to-face, and with unknown recipients are considered high risk and require enhanced due diligence (Financial Action Task Force, 2022). At the same time, FATF Recommendations state that "financial products or services that provide appropriately defined and limited services to certain types of customers, to increase access for financial inclusion purposes are lower risks" (Financial Action Task Force, 2022) and entitle supervising authorities to conduct simplified due diligence.

It is submitted that unverified e-wallets occupy the high and low-risk penumbras, as shown by the diagram below.

Figure 1

Penumbras Occupied by E-Wallet Accounts about the Level of Risks.



Unverified e-wallets are inherently high risk. They exist under cash-intensive business models and involve anonymous accounts, which are used for non-face-to-face transactions by persons who may or may not be strangers. However, as mentioned in this paper, the onboarding of the unbanked and the underbanked are crucial for financial inclusion purposes — and this is the motivating factor behind BSP's decision to onboard unverified e-wallets. The question, therefore, is — should the Philippines adopt the FATF's enhanced or simplified CDD on unverified e-wallets? In its Mutual Evaluation Report in October 2019, the Asia/Pacific Group on Money Laundering (APG) made the following observation:

Authorities have implemented some simplified measures to improve financial inclusion. This includes products in the [Money Service Businesses (MSB)] and rural bank sectors. Since higher ML/TF risks have been identified in the MSB sector, more detailed assessments of financial inclusion products have been included in both [National Risk Assessments]. In essence, the Philippines seeks a balance between financial inclusion and ML/TF risk mitigation and management in line with BSP's strategic goals in promoting financial inclusion. For example, the BSP issued a circular 50, which requires all BSP-covered persons, including MSBs, to formulate a risk-based and tiered customer acceptance, identification, and retention policy that involves reduced CDD for potentially low-risk clients and enhanced CDD for higher-risk accounts. (Asia/Pacific Group on Money Laundering, 2019).

Admittedly, the most important niche that EMIs were able to fill in the gap left by the limited reach of banking infrastructure in the country (Hasnain et al., 2016). The Philippines has 101 million people (Razon, 2017), 53% of which live in rural areas, and 21.6% live below the national poverty level (World Bank, 2019). The underserved segment is primarily comprised of two groups: (a) the unbanked, who do not have any relationship with financial institutions, and

(b) the underbanked, who have a basic but insufficient relationship with financial institutions (Razon, 2020). In this regard, mobile phones have proven to be powerful means to deliver financial services to the underserved segments of society and to achieve financial inclusion (Razon, 2020).

Nevertheless, it could hardly be argued that the EMI's neglect to verify the fraudster's account unduly exposed the victim to danger and, consequently, injury. Had the EMI verified the account, it could have determined if the registrant was fictitious and, if so, denied the account application outright. Consequently, the unverified user would have needed to have the opportunity to use the EMI's ecosystem for his or her fraudulent scheme.

Sadly, unverified e-wallet accounts could still participate in an EMI ecosystem under the present state of things. Although unverified e-wallet accounts usually could neither encash nor send money, unverified e-wallet users could still dispose of the e-money received by purchasing goods from merchant stores. Once the e-money is spent, the user of the unverified account will dispose of the prepaid SIM card to which the e-account is tethered. Since Philippine law does not require users of pre-paid sim cards to register their identities with the telecommunications provider, the fraudster's anonymity is preserved.

The Philippine Constitution provides that the "State shall protect consumers from trade malpractices and substandard or hazardous products" (PHIL. CONST. art. XVI, §9.) However, to this day, no law comprehensively addresses financial consumer rights in e-money transactions. The Electronic Commerce Act of 2000 focuses on the punishment of "hacking," "piracy," and the like and recognizes "electronic data message," "electronic signature," and "electronic documents" as admissible pieces of evidence (Electronic Commerce Act, 2000).

At best, the BSP has issued Financial Consumer Protection Framework under BSP Circular No. 857, s. 2014, (Bangko Sentral ng Pilipinas, 2014) as amended by BSP Circular No. 890, s. 2015, (Bangko Sentral ng Pilipinas, 2015) — which was later incorporated into MORNBFI as Sections 4401s and 4402s (BSP MORNBFI, 2016) — to "provide policy directions in the areas of money, banking, and credit" and "to promote "broad and convenient access to high-quality financial services and consider the interest of the general public" (The New Central Bank Act, 2018). While the framework does not define what electronic consumer rights are per se, it delineates BSP's "guidelines and expectations for BSP-Supervised Financial Institutions (BSFI)." Section 4402S.1 of the MORNBFI requires EMIs to provide consumers with (a) a reasonable understanding of its product and services and (b) ready access to information that accurately represents the service's benefits and risks during the key stages of the relationship.

The question, therefore, is: can an e-money sender file a consumer complaint against an EMI for failing to verify the fraudster's e-wallet account? The answer appears to be negative. The Financial Consumer Protection Framework is simply a policy directive for EMIs. The framework only requires BSFIs to "carefully devise, implement, and monitor a Consumer Protection Risk Management System (CPRMS) that provides the foundation for ensuring the BSFI's adherence to consumer protection standards of conduct and compliance with consumer protection laws, rules, and regulations." (BSP MORNBFI, 2016).

The BSP's policy-based approach is a far cry from the Joint DTI-DOH-DA Administrative Order No. 01, series of 2008. More than policy direction, the Administrative Order's Section 5(2) mandates "retailers, sellers, distributors, suppliers or manufacturers engaged in electronic commerce with consumers [to] provide fair, accurate, clear and easily accessible

information sufficient to enable consumers to make an informed decision whether or not to enter into a transaction." The Administrative Order outlines the procedure to file complaints against the seller/provider and incorporates the penalties under the Consumer Act and the e-Commerce Act (R.A. 7394 through 8792, 2008). In contrast, the Financial Consumer Protection Framework can only do as far as subject non-compliant BSFIs to enforcement actions (BSP MORNBFI, 2016) which, although detrimental to the BSFI's business, do not directly vindicate consumer rights. Unfortunately, even though the Consumer Act is broad enough to consider an e-wallet user as a consumer (Consumer Act, 1991) and as a product or service, e-wallet consumers cannot find refuge under the Administrative Order since it only concerns products regulated by the Department of Health, the Department of Agriculture, and the Department of Trade and Industry (R.A. 7394 through R.A. 8792, 2008).

In light of the convoluted and inconsistent consumer protection frameworks of EMIs, a user that has fallen victim to a crime facilitated through EMI platforms will be constrained to indicate his or her rights by resorting to court action against the fraudster. With this, the following questions arise: first, whether fraud victims, sans court processes, have a right to demand EMIs to disclose the personal data of e-wallet users who had defrauded them; and second, whether EMIs must ensure that the data it discloses to the victims accurately reflect the identity of its e-wallet users.

The first issue is resolved in the affirmative but qualified. The Data Privacy Act of 2012 (DPA) entitles fraud victims to demand disclosure of personal information controllers (PICs) or personal information processors (PIPs) (BGM v IPP, NPC-19-653 [2020]). In the December 2020 case of BGM v. IPP (NPC-19-653 [2020]), the National Privacy Commission ordered the payment platform to provide the complainant with the fraudster’s personal information in

compliance with Section 16(c)(3) of the DPA. The NPC ruled that the EMI's "requirement of compelling the complainant to produce a court order before the release of the requested information creates a high barrier that effectively impedes the rights vested by the [DPA] to the latter as a data subject." The NPC stressed, however, that having a legitimate purpose or some other lawful criteria to process does not mean that PICs must grant all requests to access by the data subjects. Such requests should be evaluated on a case-to-case basis. They must always be subject to the PIC's guidelines for the release of such information (BGM v IPP, NPC-19-653 [2020]), not the least of which is the proportionality principle which requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive about a declared and specified purpose.

It is worth noting, however, that the NPC's grant of the disclosure request in BGM v. IPP was based on the complainant's right as a data subject under Section 16(c)(3) of the Data Privacy Act of 2012. This meant that the case readily applies where both the requesting party and fraudster are data subjects of the same EMI. It remains unsettled whether the BGM v. IPP ruling applies if the victim transferred e-money from another EMI or e-payment provider.

Anent the second issue, Section 31 of the Data Privacy Act of 2012 (DPA) punishes the act of malicious disclosure, which is committed, among other things, when the Personal Information Provider or Controller, acting with malice and bad faith, discloses unwarranted or false information. The DPA does not define "unwarranted" information. Taken in its ordinary meaning, "unwarranted" is synonymous with "unjustified" or "lacking adequate or official support" (Merriam-Webster Dictionary, 2022). The second type of malicious data is "false information." It must be noted that unverified data is not tantamount to false data. "Unverified" is "unsubstantiated" (Merriam Webster Dictionary, 2022), whereas "false" means "not genuine or

untrue" (Merriam Webster Dictionary, 2022). If and when verified, what used to be unverified will prove to be true or false. In contrast, inherently false data is only confirmed to be untrue upon verification. In either case, verification is a necessary complement to disclosing the truth.

From this perspective, an EMI's criminal liability for malicious disclosure rests on its knowledge that the information it disclosed is false. Therefore, the question is, do EMIs have the duty to know whether the information it is about to disclose is false? The European Union General Data Protection Regulation (GDPR) resolves this in the affirmative. While the provisions of the GDPR and their interpretation are not controlling in Philippine jurisdiction, the NPC has, on various occasions, looked to the GDPR for guidance in its application of Philippine data privacy laws (National Privacy Commission, 2020).

Article 5 of the GDPR states that personal data "shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay." The closest counterpart of GDPR's Section 5 in the Philippines Data Privacy Act is Section 11 (c), which states that personal information must be: "accurate, relevant and, where necessary for purposes for which it is to be used the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted."

Compared to the GDPR, two key phrases are missing in Section 11 (c) of the Data Privacy Act of 2012: "every reasonable step must be taken to ensure,'" and "without delay." The absence of these phrases is consequential and could support the argument that, unlike the GDPR, the Data Privacy Act of 2012 does not impose PICs/PIPs, including EMIs, a positive and continuing duty to "ensure" that the data they possess is accurate.

Conclusion

This paper concludes that in operation, an EMI's non-identification and non-verification of e-wallet accounts are allowed as part of RDD. This contradicts the express provisions of the Anti-Money Laundering Act of 2001, which expressly prohibits anonymous and fictitious accounts. Under FATF Recommendation 10 on customer due diligence, onboarding unverified e-wallet accounts could occupy the high-risk and low-risk penumbras, depending on various factors. Seeking a balance between financial inclusion and money-laundering risks is a challenging task. Regardless of whether EMIs adopt enhanced or simplified CDD measures, such measures must be consistent with the provisions of the law and FATF Recommendations.

This paper likewise found that EMIs must disclose information on their users under the circumstances contemplated under the Data Privacy Act of 2012. The NPC ruled that EMIs shall disclose information for fraud investigation based on the requesting party's "right to access" as a data subject and that no court order is needed for such disclosure. However, the ruling only applies in cases where both senders and receivers are consumers/data subjects of the same EMI and not concerning third-party senders transacting through the National Payment and Retail System.

Ultimately, it seems more practical for the victim to initiate a civil or criminal activity directly. Under Rule 3, Section 14 of the Revised Rules of Court, the victim-plaintiff may resort to discovery procedures and subpoena the EMI to produce all traffic data concerning the e-wallet transaction in the hopes of pinpointing where the fraudster transacted and other important information leading to his identity. Unfortunately, the plaintiff in the civil case will have to shoulder considerable expense in hiring technical experts to decipher the data and testify in court. From this vantage point, a civil case may prove to time costly and impractical, especially

if the amount defrauded is small. Given this, victims may be better to request law enforcement agencies to prosecute a criminal action and secure from the court a cyber warrant to disclose Computer Data. However, practical considerations such as the clogged dockets of law enforcement agencies and the protracted steps involved in prosecuting offenses may also discourage private offended parties from pursuing a criminal case altogether.

Recommendations

There is a well-founded fear that premature or over-regulation of fast-paced industries such as FinTech may stifle growth and impede its ongoing expansion and development (Smith, n.d.), which are essential components of financial inclusion (International Monetary Fund World Bank, 2018). However, authorities must recognize the cybercrime and anti-money laundering gaps resulting from insufficient or misaligned regulations. Allowing the market to self-regulate would only increase the risks identified (Soriano et al., 2019). Regulators must therefore strike a balance when tackling the issues brought on by FinTech in order to maintain consumer confidence and promote the sandboxing of EMIs. It is advised that authorities implement temporary precautions that will alert the general public to the dangers of using an unverified e-wallet in place of strict regulatory legislation. In the case of BSP, the author recommends that it issue regulations that will mandate EMIs:

To prompt e-wallet users that the e-wallet account they are sending or receiving e-money from needs to be verified.

To jointly administer the warning mentioned above protocols with other operators within the National Retail Payment System.

With the said regulations in place, EMIs will have a clear obligation to inform users that the person they are transacting with is using an unverified account and afford the sender a

meaningful opportunity to inquire further on the recipient's identity or decide not to proceed with the transaction at all. The regulation shall likewise compel EMIs to work with other operators within the National Payment System, i.e., Banks, Non-Bank Financial Institutions, Money Service Businesses, and other EMIs, to develop and implement protocols that will warn end-users. More than educating consumers, these regulations will ensure consumer confidence and curb crimes committed through unverified e-wallet accounts.

References

An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use Thereof, and Other Purposes [Electronic Commerce Act of 2000], (Ph). Republic Act No. 8792 (2000).

An Act for the Regulation and Supervision of Payment Systems, (Ph). Republic Act No. 11127 (2018).

An Act further strengthening the Anti-Money Laundering Law, amending for Republic Act No. 9160, otherwise known as the "Anti-Money Laundering Act of 2001", as amended (Ph). Republic Act No. 10365, § 4 (2013). http://www.amlc.gov.ph/laws/money-laundering/2015-10-16-02-50-56/republic-act-10365

Asia/Pacific Group on Money Laundering (2019, October). Anti-money laundering and counter-terrorist financing measures: Philippines Mutual Evaluation Report, at 46, ¶105. http://www.apgml.org/members-and-observers/members/member-documents.aspx?m=63a7bacb-daa2-47ee-9ac3-1e27a9eff73f

Arner, D. et al., (2019, December 19). The Evolution of FinTech: A New Post-Crisis Paradigm. 47 GEO.J. INT'L. 1271.

Balinbin, A. (2021, March 8). Cybercrime to increase further as transactions shift online. BUSINESSWORLD. https://www.bworldonline.com/cybercrime-to-increase-further-as-transactions-shift-online

Bangko Sentral ng Pilipinas (2009, March 9). Guidelines Governing the Issuance of Electronic Money (E-Money) and the Operations of Electronic Money Issuers (EMI), BSP Circular No. 649.

Bangko Sentral ng Pilipinas (2015, 2 November). Amendments to the Manual of Regulations for Banks and Manual of Regulations for Non-Bank Financial Institutions, BSP Circular No. 890, s. 2015.

Bangko Sentral ng Pilipinas (2018). Manual of Regulation for Non-Bank Financial Institutions. https://morb.bsp.gov.ph/702-issuance-and-operations-of-electronic-money/

Bangko Sentral ng Pilipinas (2016). Manual of Regulation for Non-Bank Financial Institutions. https://www.bsp.gov.ph/Regulations/MORB/2016_01MORNBFI2.pdf

Bangko Sentral ng Pilipinas (2017, November 2). Adoption of National Retail Payment System (NRPS) Framework, BSP Circ. No. 980, s. 2017.

Bangko Sentral ng Pilpinas (2014, 21 November). BSP Regulations on Financial Consumer Protection, BSP Circular No. 857, s. 2014

Beltran, B. (2022, February 11). The growing momentum of Philippine fintech. The Global Compliance News. https://www.globalcompliancenews.com/2022/09/22/fintech-philippines_09222022/

BGM v. IPP, NPC Case No. 19-653, (NPC), (2020).

Cantorias, M. (n.d.). Anti-Money Laundering/Combating Financing of Terrorism: A Philippine Perspective on a Donor-Driven Initiative. https://arellanolaw.edu/alpr/v10n1c.pdf

Coins.ph. (n.d.). How can I increase my daily transaction limits? https://support.coins.ph/hc/en-us/articles/201305154-How-can-I-increase-my-daily-transaction-limits-

Consumer Act of the Philippines, (Ph). Republic Act No. 7394, §4(n) (1991). https://www.officialgazette.gov.ph/1992/04/13/republic-act-no-7394-s-1992/

Esquire Philippines. (2020, November 15). Scam Alert: Fake Typhoon Victims Are Reportedly Asking for Cash Donations. https://www.esquiremag.ph/politics/news/fake-typhoon-victims-are-reportedly-asking-for-cash-donations-a00203-20201115.

Tookitaki. (2022, August 17). E-wallets and Anti-Money Laundering in the Philippines. https://www.tookitaki.com/blog/news-views/e-wallets-and-anti-money-laundering-in-the-philippines

Philippine Daily Inquirer. (2022, March 10). E-wallets and illegal activities. https://opinion.inquirer.net/150851/e-wallets-and-illegal-activities

Financial Action Task Force. (2022). About. https://www.fatf-gafi.org/about/

Financial Action Task Force. (2022). Recommendation 10: Customer Due Diligence. https://www.cfatf-gafic.org/index.php/documents/fatf-40r/376-fatf-recommendation-10-customer-due-diligence

Fintech News Philippines. (2021, December 22). Fintech in the Philippines: 2021 in Review. https://fintechnews.ph/54878/fintechphilippines/fintech-in-the-philippines-2021-in-review/

GCash (2021). Benefits of Verification. https://help.gcash.com/hc/en-us/articles/360017721953-Why-do-I-need-to-get-Verified-

Grab. (2019, 24 June). Activate Your GrabPay Basic Wallet by Confirming Your Identity. https://www.grab.com/ph/blog/activate-your-grabpay-basic-wallet/

Hasnain, et al. (2016, 23 June). Mobile money in the Philippines: Market conditions drive innovation with Smart Money and Gcash. GSMA. https://www.gsma.com/mobilefordevelopment/programme/mobile-money/mobile-money-philippines-market-conditions-drive-innovation-smart-money-GCash-philippines-becoming-mobile-money-innovation-hub/

International Trade Administration. (2021, September 11). Philippines - Country Commercial Guide. https://www.trade.gov/country-commercial-guides/philippines-ecommerce

Jeans, N. (2016). Risk-based approach to KYC. Thomson Reuters. https://blogs.thomsonreuters.com/answerson/kyc-risk-based-approach/

Lopez, D. (2020, November 20). Philippines Sees Surge in Financial Scams During Pandemic. BLOOMBERG. https://www.bloombergquint.com/onweb/philippines-sees-surge-in-financial-scams-during-pandemic

Manila Standard. (2021, 11 February). P.H. is on the verge of a coinless society. https://manilastandard.net/spotlight/manila-standard-34th-anniversary-in-support-of-economic-reopening/346667/ph-on-the-verge-of-coinless-society.html

M.Pat. (2021, February 3). Re: Tracing Scammer using Gcash account. Freedom of Information Philippines. https://www.foi.gov.ph/requests/aglzfmVmb2ktcGhyHQsSB0NvbnRlbnQiEE5CSS0zMDkwODg5NTMzNDEM

Manila Standard. (2021, 11 February). P.H. is on the verge of a coinless society. The Manila Standard. https://manilastandard.net/spotlight/manila-standard-34th-anniversary-in-support-of-economic-reopening/346667/ph-on-the-verge-of-coinless-society.html

Manual of Regulation for Non-Bank Financial Institutions (MORNBFI) as Sections 4642N to 4642N.7

Merriam Webster Dictionary, Retrieved from at https://www.merriam-webster.com/dictionary/false

Merriam Webster Dictionary, Retrieved from at https://www.merriam-webster.com/dictionary/unverified

Merriam Webster Dictionary, Retrieved from at https://www.merriam-webster.com/dictionary/unwarranted

National Privacy Commission. (2020, 26 November). Privacy Policy Office Advisory Opinion No. 2020-050 Re: Disclosure by Fintech, Digital Payments Platforms and Telecommunications Entities of Personal Data for Fraud Investigation. https://www.privacy.gov.ph/wp-content/uploads/2020/12/Redacted-Advisory-Opinion-No.-2020-050.pdf

PayMaya. (2020, April 22). What are the Transaction Limits of my Maya Account? https://support.maya.ph/s/article/What-are-the-transaction-limits-of-my-PayMaya-account Phil. Const. art. XVI, §9.

Quintero, D., Ilas-Panganiban, P., & Navarro, K. (2022, September 22). Philippines: Fintech in the Philippines 2022. Global Compliance News. https://www.globalcompliancenews.com/2022/09/22/fintech-philippines_09222022/

Razon, A. (2020). Towards Financial Inclusion Through Digital Financial Services: Examining the Impact of the 'Notice and Consent' Privacy Mechanism, 11 Case W. Res. J.L. Tech. & Internet 50, 101 (citing Bangko Sentral ng Pilipinas, Financial Inclusion Initiatives 2017). https://perma.cc/G45C-ENXW].

Revised Rules and Regulations Implementing the Anti-Money Laundering Act of 2001, rule 18, §11.2. (2018). http://www.amlc.gov.ph/images/PDFs/FINAL2018%20IRR.pdf

Rules and Regulations for Consumer Protection in a Transaction Covered by the Consumer Act of the Philippines (Republic Act No. 7394) Through Electronic Means Under the E-Commerce Act (Republic Act No. 8792), §1 (2000). https://www.lawphil.net/statutes/repacts/ra2000/ra_8792_2000.html

Rules and Regulations for Consumer Protection in a Transaction Covered by the Consumer Act of the Philippines (Republic Act No. 7394) Through Electronic Means Under the E-Commerce Act (Republic Act No. 8792), §9 (2000). https://www.lawphil.net/statutes/repacts/ra2000/ra_8792_2000.html

Rules and Regulations for Consumer Protection in a Transaction Covered by the Consumer Act of the Philippines (Republic Act No. 7394) Through Electronic Means Under the E-Commerce Act (Republic Act No. 8792), Joint DTI-DOH-DA Admin. Order No. 1, s. 2008 (2008).

Rules and Regulations for Consumer Protection in a Transaction Covered by the Consumer Act of the Philippines (Republic Act No. 7394) Through Electronic Means Under the E-Commerce Act (Republic Act No. 8792), Joint DTI-DOH-DA Admin. Order No. 1, s. 2008 (2008). https://ecommerce.dti.gov.ph/related-laws-policy-issuance/

Rules and Regulations Implementing the Anti-Money Laundering Act of 2001, Republic Act No. 9160, rule 9.1.c (2002). https://www.bsp.gov.ph/Regulations/Banking%20Laws/RA9194_IRR.pdf

Rules and Regulations Implementing the Anti-Money Laundering Act of 2001, Republic Act No. 9160, rule 9.1.a (2002). https://www.bsp.gov.ph/Regulations/Banking%20Laws/RA9194_IRR.pdf

Salerno, A. (September 2021). Regulating the Fintech Revolution: How Regulators can adapt to Twenty-First Century Financial Technology. https://annualsurveyofamericanlaw.org/wp-content/uploads/2021/09/75.2-Salerno.pdf

Salud, J. (2021). Take My E-money: The Legal Framework of Electronic Money, and the Anti-Money Laundering, Consumer Protection and Data Protection Regulatory Issues that Arise from the Onboarding of Unverified E-Wallet Accounts in the Philippines. [Unpublished Thesis Paper for Master of Law] Ateneo de Manila University School of Law

Santiago, A. (2021, April). An Overview of the Philippines' E-Money Boom. YCP Solidance. https://ycpsolidiance.com/article/an-overview-of-the-philippines-e-money-boom

ShopeePay. (2021, 5 July). ShopeePay Terms of Service. https://shopee.ph/docs/6907

Smith, R. (n.d.). Do Regulatory Questions Threaten the Rise of Fintech? Fintech Weekly. https://fintechweekly.com/magazine/articles/do-regulatory-questions-threaten-the-rise-of-fintech

Soriano, M., et al. (n.d.). The ASEAN FinTech Ecosystem Benchmarking Study. https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-ccaf-asean-fintech-ecosystem-benchmarking-study.pdf

The New Central Bank Act, (Ph). Republic Act No. 11211 (2018).

TrueMoney. (2021, 14 June). Terms and Conditions. https://truemoney.com.ph/2020/05/05/terms-and-conditions/

Tupas, E. (2020, October 25). Online Scams Spike During Quarantine. PHIL. STAR. https://www.philstar.com/headlines/2020/10/25/2052110/online-scams-spike-during-quarantine [Source: https://studycrumb.com/alphabetizer]

United Nations. (n.d.). Transforming our world: the 2030 Agenda for Sustainable Development. https://sdgs.un.org/2030agenda

United Nations. (2020, August). United Nations Task Force on Digital Financing of Sustainable Development Goals, Peoples' Money: Harnessing Digitalization to Finance a Sustainable Future. https://www.un.org/sites/un2.un.org/files/df_task_force_-_full_report_-_aug_2020.pdf

World Bank & International Monetary Fund, the Bali FinTech Agenda — Chapeau Paper. (2018, September 19) at ¶1. http://documents1.worldbank.org/curated/en/390701539097118625/pdf/130563-BR-PUBLIC-on-10-11-18-2-30-AM-BFA-2018-Sep-Bali-Fintech-Agenda-Board-Paper.pdf