Issue No. 27
iAMLatest
Surveillance Report on AML/CFT Trends
Financial System Integrity Department
Bangko Sentral ng Pilipinas

ML/TF Risks Related to New Payment Methods

Digital innovation has considerably transformed the delivery of financial system landscape. It has not only resulted in the development of new financial products and services but also reshaped customer behavior and the regulatory environment. This, however, yielded emerging ML/TF risks and typologies posed by new payment methods (NPM) or new payment products and services (NPPS)[1] such as prepaid cards, mobile payments, and internet payment services [e.g., digital wallets, digital currencies, virtual currencies, or electronic money (e-money)][2].

The Financial Action Task Force, in its 2013 Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services, has identified several inherent risks associated with NPM and NPPS, which include anonymity of its customers, possibility of "non face-to-face" business relationships, cross-border access/geographical reach, and variety in methods of funding (e.g., anonymous or third party funding). Measures to mitigate the risks of ML and TF in NPMs, include customer due diligence (CDD), loading, value and geographical limits, source of funding, transaction monitoring/reporting and record keeping, among others[3]. Continued vigilance is necessary to further understand, identify, and assess the impact of NPM and other evolving technologies on financial products and services without compromising the achievement of financial inclusion objectives.

In this regard, BSP-supervised financial institutions should identify and assess the ML/TF risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products, and should take appropriate measures to manage and mitigate those risks[4].

[1] NPPS are considered to be new and innovative payment products and services that offer an alternative to traditional financial services. NPPS include a variety of products and services that involve new ways of initiating payments through, or extending the reach of, traditional retail electronic payment systems, as well as products that do not rely on traditional systems to transfer value between individuals or organizations.
[2] Guidance for Risk Based Approach on Prepaid Cards, Mobile Payments, and Internet-based Payment Services (June 2013), p. 4, 10, 14 (https://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf)
[3] Ibid.
[4] https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

LAWS AND REGULATIONS

Excerpts from Section 911/911-Q of the Manual of Regulations for Banks (MORB)/Manual of Regulations for Non-Bank Financial Institutions (MORNBFI)*

https://www.bsp.gov.ph/Regulations/MORB/2020MORB.pdf

New products and business practices risk assessment. Covered persons are required to identify and assess the ML/TF risks that may arise in relation to the development of new products and new business practices, including new delivery mechanisms, and the use of new or developing technologies for both new and pre-existing products. Such risk assessment should be an integral part of product or service development process and should take place prior to the launch of the new products, business practices or the use of new or developing technologies. Covered persons should take appropriate measures to manage and mitigate the identified risks.

**Similar requirements cited in Rule 19, Section 5 (New Technologies) of the 2018 Implementing Rules and Regulations of Republic Act (R.A.) No. 9160, otherwise known as The Anti-Money Laundering Act of 2001, as amended [January 2021 Amendment];*
Source: http://www.amlc.gov.ph/images/PDFs/2018%20IRR%20(2021%20JAN%20AMENDMENT).pdf

Excerpts from the Recommended Control Measures Against Cyber Fraud and Attacks on Retail Electronic Payments and Financial Services (EPFS)

BSP Memorandum No. M-2022-015 dated 22 March 2022

https://www.bsp.gov.ph/Regulations/Issuances/2022/M-2022-015.pdf

- ✓ Removal of clickable links in emails or SMS sent to retail customers followed by an information campaign that the BSFI will no longer be sending clickable links.
- ✓ Customer notification through existing mobile or email whenever there is a request to change a customer's account credentials.
- ✓ Mandatory fund transfer transaction notification for transactions exceeding a predefined amount.
- ✓ Holding period or delay before activation of a new soft token on a mobile device.
- ✓ Cooling-off period before the implementation of requests for key account changes.
- ✓ Personalized SMS/Email OTP messages for device registration, fund transfer, and profile update.
- ✓ Restriction to any BSFI officer/representative from manually obtaining or inquiring about critical authentication information.
- ✓ Creation of dedicated and well-resourced customer assistance teams that deal with feedback on potential fraud cases on a priority basis.
- ✓ Conduct of regular customer education campaigns against online scam and phishing schemes with mechanisms to monitor their effectiveness and relevance.
- ✓ Adoption of strong fraud surveillance mechanisms to ensure prompt responses in dealing with the growing threat of online scams.

Excerpts from the Guidelines on Sound Risk Management Practices in Dealings with Operators of Payment Systems (OPS) and Non-Bank Electronic Money Issuers (Non-Bank EMIs)

BSP Memorandum No. M-2021-021 dated 5 April 2021

https://www.bsp.gov.ph/Regulations/Issuances/2021/M-2021-021.pdf

- ✓ Perform appropriate assessment of entities based on observable business activities and transactions indicating that such entities are OPS or non-bank EMIs required to register with the BSP or licensed by the BSP, respectively.
- ✓ Deal only with BSP-registered OPS and/or duly-licensed non-bank EMIs.
- ✓ Perform appropriate CDD when dealing with BSP-registered OPS or duly-licensed non-bank EMIs. Where a BSFI is unable to comply with the relevant CDD measures, it shall (a) not open the account, not commence business relations, refuse to perform the transaction, or terminate the business relationship; and (b) consider filing a suspicious transaction report (STR) in relation to the customer pursuant to Section 921/921-Q of the MORB/MORNBFI.
- ✓ Conduct appropriate risk assessment of the OPS/non-bank EMIs to identify, understand, and assess risks arising from the OPS/non-bank EMIs and apply appropriate due diligence depending on risk profile considering relevant factors.
- ✓ Perform continuing account transaction monitoring.

Excerpts from the Amendments to Regulations on Information Technology Risk Management

BSP Circular 1140, Series of 2022, dated 24 March 2022

https://www.bsp.gov.ph/Regulations/Issuances/2022/1140.pdf

Implementation of an automated and real time fraud monitoring and detection systems. BSFIs must implement automated and real-time fraud monitoring and detection systems to identify and block suspicious or fraudulent online transactions. The expected sophistication and capabilities of BSFIs' fraud monitoring systems (FMS) should be ***commensurate to the risks associated with their digital financial and payment platforms***. The FMS should be ***constantly calibrated to be able to process surges in transactions, collectively analyze customer profiles/behavior, and detect new fraud patterns***. To ensure robustness and effectiveness in early detection and prevention of fraudulent and suspicious activities, ***it is optimal that the FMS is able to collect, monitor, and analyze transactions from all channels***. **Moreover, the *FMS and the AML systems should be linked or integrated*** to have a cohesive and comprehensive financial crime prevention system.

Consumer awareness. BSFIs should pay special attention to the provision of easy to understand and prominent advice to its customers on security precautions for e-services. As an integral part of their customer onboarding process, BSFIs shall ensure that their clients have undertaken a pre-requisite consumer education course/program on the safe and secure use of electronic payment and financial services (EPFS), including the associated risks. To effectively capture the customer's attention and interest and reinforce their awareness and understanding of risks, BSFIs should explore the use of interactive platforms/materials such as but not limited to video clips, online quizzes, infographics, etc. BSFIs shall likewise adopt a program aimed at promoting continuing awareness and constantly reminding its clients on the safe and secure use of EPFS, including the associated risks.

LOCAL NEWS/PUBLICATIONS

E-wallets and illegal activities

Author: Philippine Daily Inquirer
Date Published: 10 March 2022 / Accessed on: 17 August 2022
Source (excerpts from): https://opinion.inquirer.net/150851/e-wallets-and-illegal-activities

Online payment platforms have come under scrutiny by legislators and regulators amid concerns these can be used for vote-buying, online *sabong* and other gambling activities, money laundering, and even terrorism.

Fortunately, the BSP and the Anti-Money Laundering Council (AMLC) are very much aware of these dangers and have, for example, directed banks and other financial services providers to shore up their cybersecurity systems to prevent accounts from being unlawfully accessed and compromised.

The AMLC joined the BSP in calling the attention of the financial system to possible proliferation of digital vote-buying and selling schemes and listed down "red flags" or suspicious behaviors, including coordinated or structured deposits and money transfers; significant or large transactions occurring in a short period of time; unjustified large cash deposits and withdrawals, and transactions deemed inconsistent with the customer's financial profile or declared business.

The private sector has responded to the challenge to help stamp out these illegal activities with the launch of an advocacy campaign preaching the responsible use of digital payment platforms. They have likewise assured the BSP and AMLC that robust security systems are in place to help prevent crime perpetrated online.

Such partnership is reassuring to customers who are indeed wary of the risks but have at the same time realized the benefits of using financial technology such as mobile wallets that have allowed more Filipinos to access vital financial services. That fragile trust can be strengthened by constant vigilance, investments in safety and procedures, and a grim determination to ensure that criminal activities such as money laundering will have no place in these now-indispensable online financial system.

Philippines remains top target for hackers

Author: Ehda M. Dagooc | Date Published: 29 June 2022 / Accessed on: 25 August 2022
Source (excerpts from): https://www.philstar.com/the-freeman/cebu-business/2022/06/29/2191736/philippines-remains-top-target-hackers

The Philippines remains an easy target for hackers as it ranked the highest in terms of attracting phishing attempts in Southeast Asia. A report released by cybersecurity company Kaspersky revealed that 10 or 68.95 percent phishing attempts targeted finance-related transactions in the Philippines from February to April this year, based on anonymized data voluntarily provided by Kaspersky customers. The cybersecurity company detected and blocked phishing attacks against three financial categories namely, banks, e-commerce stores and payment system. Statistics from Kaspersky Security Network (KSN) revealed that phishing attempts in the Philippines is higher than in Indonesia (65.90 percent), Singapore (55.67 percent), Thailand (55.63 percent), Malaysia (50.58 percent) and Vietnam (36.12 percent).

In all three (3) finance categories during the same three-month period, Kaspersky data showed that there were one in two (58.50 percent) phishing attempts against payment systems in the country such as credit cards, debit cards, and mobile payment apps or e-wallets. This number is the highest among countries in South East Asia.

"Alongside the increased adoption in digital transactions here in Southeast Asia, we also see the rise of "Super Apps" in the region. These are the mobile applications that combine all popular monetary functions including e-banking, mobile wallets, online shopping, insurance, travel bookings, and even investments. Putting our data and digital money in one basket can trigger an aftermath snowball, with the impact of a phishing attack swelling at an unforeseeable rate," said Yeo Siang Tiong, General Manager for Southeast Asia at Kaspersky.

"It is known that cybercriminals follow the money trail, so it is important for banks, app developers, and service providers to integrate cybersecurity from the beginning of application development. We expect hackers to target the rising Super Apps, both its infrastructure and its users through social engineering attacks. We urge all fintech companies to deploy a secure-by-design approach in their systems and to continuously provide proactive education for their users in this period where phishing attacks continue to thrive," added Yeo.

Banks and service providers need to ensure a security team (or security experts) that will be able to ensure that cyber defense infrastructure is updated and will be able to provide support in the event of a cyberattack.

INTERNATIONAL NEWS/ PUBLICATIONS, TYPOLOGIES & BEST PRACTICES

In the New Normal of Payments, What are the Top AML Risks?

Author: Comply Advantage
Date Published: Originally published 6 November 2020; Updated 5 May 2022 / Accessed on: 27 July 2022
Source (excerpts from): https://complyadvantage.com/insights/aml-cft-risks/

The COVID-19 crisis has accelerated the shift to the "new normal" of payments. Along with it comes new anti-money laundering (AML) and countering the financing of terrorism (CFT) risks for e-payment providers. Below are six (6) AML/CFT areas to consider under this new environment.

RISE OF E-COMMERCE

Social distancing guidelines and stay-at-home orders have led to a surge in online spending and, as a result, cashless payment options. The accessibility of online marketplaces makes it easy to set up a fake online store as a front or pass-through company, which increases AML/CFT risk. In China, for instance, money launderers have been placing fake e-Commerce purchases to move money to offshore gambling sites.

Aside from providing consumers with a safe and secure platform to pay for their online purchases, e-payment providers now find themselves in the position to be the first line of defense against money laundering and fraudulent transactions. For starters, this means doing customer due diligence (CDD) checks throughout the lifetime of each client and offering tokenization, among other measures.

E-WALLETS AND THEIR AML RISKS

The surge in e-commerce activity in Asia has also led to increased adoption of e-Wallets. In the Philippines, where consumers have historically paid for online purchases through cash on delivery (COD), COVID-19 has forced consumers to turn to virtual wallets. e-Wallet providers can protect their platform by implementing transaction monitoring for AML, identifying discrepancies in customer identity during registration, and flagging frequent and rapid cash withdrawals of funds moved between accounts

PREPAID CARDS

The accessibility of prepaid cards and the relative anonymity they afford (i.e., no need to link to a bank account) makes them a prime target for all three money laundering (ML) stages: placement, layering, and integration. A common ML tactic with prepaid cards is "smurfing" where multiple cards are loaded with amounts below the KYC (know your customer) threshold. Prepaid card providers can fix this problem simply by securing their virtual card management platforms and the cards themselves more effectively. Providers can also implement measures such as limits on funding, reloading, and spending, stricter cash access controls, and limiting access within specific geographic locations.

ONLINE MONEY TRANSFERS AND AML RISKS

The rise of money transfer apps has made it even easier for money launders to move money across borders. Criminals can use 'money mules' to get other people to move money on their behalf or simply use fake identity documents to bypass CDD checks. Remittance firms must employ systems that automatically detect typical AML remittance red flag behaviors, such as suspicious remittance patterns and transfers to high-risk countries and websites. In addition, AML compliance for online remittance services should meet FATF guidelines.

ONLINE GAMING AND MICROPAYMENTS

Online games, particularly massive multiplayer online role-playing games, have long been suspected of being an under-reported avenue for ML due to their use of in-game credits—effectively a form of cryptocurrency. Criminals break down a large amount of money by purchasing in-game currency and selling these credits to gamers at a discount without triggering AML risk alerts. This scheme is known as micro laundering.

With the right transaction monitoring rules in place, game developers can implement systems to detect micro laundering. The key is to have the proper rules in the regulatory technology workflow to identify micro laundering risks. This allows the AML system to flag not just large, single transactions, but also less obvious tactics.

ESCROW SERVICES AND THEIR AML RISKS

Escrow services are used by online gig marketplaces, buy-and-sell platforms, and various types of online financial transactions, from buying a domain name to purchasing a vehicle. These services can be exploited to launder dirty money through money mules. The simplest solution against this problem is to implement KYC procedures to verify the identity of every user, seller, or buyer involved when money is held in escrow.

Best Practices for Preventing E-Payment-based AML Risks

To provide effective AML/CFT risk compliance, e-payment providers should implement a suitable automated, intelligent transaction monitoring for AML systems to analyse customer and transaction data and identify red flag activities. Automated AML data solutions not only identify risks before they become threats, but they also reduce the risk of human error and deliver ongoing compliance by adapting to global watchlist databases and legislation.

On an administrative level, e-payment providers must be proactive in ensuring they meet all licensing and registration requirements that apply to them.

Managing financial crime risk in digital payments

Author: Daniel Mikkelsen, Shreyash Rajdev, and Vasiliki Stergiou
Date Published: 24 June 2022 / Accessed on: 17 August 2022
Source (excerpts from): https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/managing-financial-crime-risk-in-digital-payments

The explosion in the number of electronic transactions is part of the electronic commerce (e-commerce) and mobile commerce (m-commerce) booms and the shift away from cash payments. Digital-payments mechanisms include cards but also recent payments innovations, such as digital wallets. This shift to digital payments is expected to continue. One unavoidable measure of the booming success of payments service providers (PSPs) is the increased risk of financial crime. Unmanaged, this risk can pose an existential threat for PSPs.

According to FATF, financial-crime incidents and failings have been on the rise throughout the pandemic. Particularly in the consumer realm, the potential for fraud has also grown with the advent of the COVID-19 pandemic. To cope, many PSPs enhanced their controls, such as transaction monitoring, while regulators updated requirements relating to remote onboarding and ongoing customer due diligence.

As PSPs rethink their approach to managing financial crime, they can apply **three (3) core design principles**.

1 Build a proportionate framework

The control framework should be proportionate to the overall business model. Organizations will have to decide which risks they are willing to accept versus those that will be outside their risk appetite.

2 Challenge the traditional control environment

PSPs can challenge the efficacy of the control environments and frameworks of traditional banks. More controls do not necessarily mean better protection from financial crime for PSPs. By identifying this tension, PSPs will be able to think more creatively and actively develop solutions both to meet regulatory requirements and support their customer experience goals.

3 Be continuously proactive toward exposures

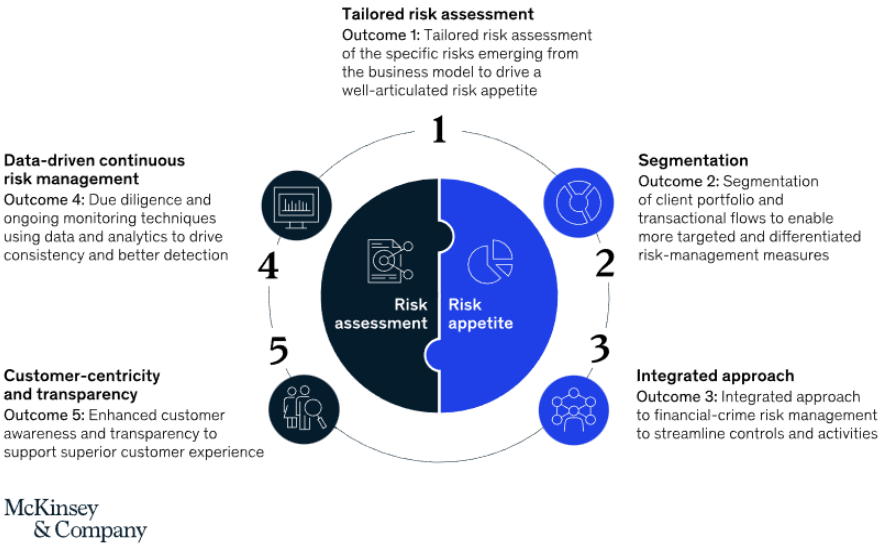
To respond effectively to their exposures, PSPs will have to anticipate risks and build protections into the design of core services and products. They must also continuously update their approach, swiftly adjusting their regular and ad hoc software releases, for example, to address the changing fraud threat landscape.

Five (5) Pillars for Managing Financial Crime Risks

1. **Tailored risk assessment driving risk appetite.** PSPs and other service providers to consumers and merchants need to identify the specific potential risks they face and build the appropriate internal infrastructure to business. Each PSP will have to consider the distinct typologies and scenarios of the financial-crime risks to which their business models are exposed.

2. **Segmented client portfolio and transactional flows**. Segmentation enables more targeted and differentiated risk management measures. Pursuing the objective of detecting and stopping prohibited transactions and bad actors often comes at high operational cost. The idea behind an appropriate risk-based approach is that PSPs should focus more comprehensively on the small percentage of potentially risky transactions and customers. To do this, institutions will need to develop more nuanced segmentation models, based on real-time, up-to-date data to enable targeted detection and a clear ranking of customers and transactions, from lowest to highest risk. The model would consider not only historical transaction data and static customer records but also forward-looking data points and external data on bad actors.

Five core pillars can shape the anti–financial crime strategy for payment service providers.



3. **Integrated, streamlined controls and activities**. PSPs are highly skilled in developing unified infrastructure and integrated teams across risk types—such as fraud, AML, sanctions, and cyber risk. PSPs have a less siloed structure in this respect than banks. They can use data from each of these related risk disciplines to inform decision making across processes.

   This may involve the use of data and controls for fraud detection and AML transaction monitoring to identify trends that suggest correlations with ML and other prohibited activities. It may also involve integrating the various anti–financial crime controls that apply to certain products or services, in order to avoid customer friction and enhance overall effectiveness.

4. **Data-driven, continuous risk management**. The use of innovative and existing technologies and data will enable PSPs to roll out continuous and targeted monitoring solutions, the design of which is informed by tailored data analysis rather than expert judgment only. PSPs should aim to design intelligent automated processes, applying machine learning and analytical approaches where they make the most sense. These tools can dramatically improve effectiveness, reducing false-positive rates and reliance on labor-intensive processes.

5. **Customer-centricity and transparency**. Stronger anti–financial crime controls need not have a negative impact on customer experience. Instead, the controls embedded in the customer journeys can enhance customer experience and trust in the PSP. Features could include faster transaction speeds and enhanced ease of interactions via digital channels, using external data and user-friendly interfaces.

Preventing Digital Payment Systems Fraud

Author: Brian Baral & Joseph Gillespie
Date Published: 4 May 2022 / Accessed on: 17 August 2022
Source (excerpts from):
https://www.acamstoday.org/preventing-digital-payment-systems-fraud

Unfortunately, the surge in digital payments has also attracted fraudsters determined to illegally profit from this trend. As providers adopt and scale digital payment capabilities to match its demand, it is critical that they prevent fraud and reduce losses while minimizing customer friction. Providers must have a good grasp of the tactics that criminals are using. These tactics fall into several key areas, including:

Peer-to-Peer Fraud

There is fraud involving popular peer-to-peer (P2P) payment apps which frequently occurs through social engineering and scams. Some of the scams include fake merchandise and fake charity donations as well as account takeovers, which involve customer information obtained through the dark web or through malicious bots. Fraudsters use stolen identity information to apply for new P2P and digital wallet accounts and then use those accounts to purchase goods and services.

Authorized Push Payment Fraud

Authorized push payment fraud is another fraudulent technique that occurs when scammers pose as legitimate businesses or government officials to trick victims into transferring funds to them through real-time digital payments.

Friendly Fraud

Friendly fraud is also on the rise. This involves a user disputing a valid transaction, or a user's mobile apps and logins being used by friends and family members without permission. A provider's security features cannot stop this type of fraud and merchants often do not have enough information to track and validate the transaction, so chargebacks typically go through successfully and merchants bear the cost of refunding the money to consumers.

How to Protect Your Digital Payments Systems

- ✓ **Use a cloud platform.** Using a cloud platform to enable robust data ingestion and enrich data from multiple sources would provide a broader spectrum of real-time data, enabling faster analysis, real-time fraud detection and more accurate fraud decisions.
- ✓ **Examine the entire customer lifecycle**. Gather centralized data intelligence holistically, in real-time, at each customer touchpoint, from application, transactions to account updates and from device data to behavioral data. This will help quickly identify evolving fraud patterns.
- ✓ **Use intelligent authentication**. Depend less on passwords and use secure, frictionless methods for intelligent customer verification and authentication. Modern-day fraud verification and authentication incorporates advanced digital technologies, such as artificial intelligence, machine learning, and biometrics (fingerprint, facial and voice recognition) as well as dynamic data for customer verification and authentication.
- ✓ **Preserve the customer experience**. Building a seamless fraud-detection process that is invisible to customers requires optimal prioritization between growth (e.g., approval rate) and fraud rate.

Payment Systems (and Trust) Are Vulnerable to Financial Crime

Author: Samantha Parish and Michael Shepard
Date Published: 17 February 2022 / Accessed on: 17 August 2022
Source (excerpts from):
https://www.forbes.com/sites/deloitte/2022/02/17/payment-systems-and-trust-are-vulnerable-to-financial-crime/?sh=36c45b6d67b3

Financial criminals aim to take advantage of increasing mobile payment traffic as companies undergo remote work, staffing changes, and other forms of pandemic-driven disruption. Those criminals are also using technologies such as robotic process automation and artificial intelligence (AI) to launch increasingly sophisticated attacks on digital channels for moving money. At the same time, relatively new, more lightly regulated payment platforms have expanded the risks associated with transactions.

Technology-driven payment service providers (PSPs) are driving many of these changes. While PSPs are not regulated as banks, they are subject to AML/CFT regulations and to laws related to bribery and other illegal payments. PSPs, or organizations who own, operate, use, or partner with a PSP, must be aware of the risks, which include financial, operational, cybersecurity, data privacy, regulatory, and legal risks.

Manage risks proactively

Given heightened risks, PSPs and organizations that use or are affiliated with them may consider upgrading their fraud and financial crime programs to adequately address threats to their systems, customers, users, partners, and reputations.

A proactive financial crime program can deploy upfront risk assessment and mitigation measures to deter bad actors and facilitate faster, deeper investigations of incidents. These programs, which should be risk-based, can provide greater comfort to senior executives, board members, customers, partners, investors, and regulators.

In addition to establishing a risk-based approach, organizations should consider the following steps:

- **Broaden the view of risk.**

A comprehensive risk assessment would encompass identity theft, account takeover, ML, fraud, bribery, corruption, and payments related to sanctions, drug and human trafficking, and labor exploitation. This assessment would seek not only to assess specific risks, but also to identify risks to brand, reputation, and trust across the enterprise.

- **Monitor potential criminal activity**

Intelligent technologies for monitoring transaction activity can generate targeted coverage and reduce false positive alerts. AI and machine learning tools can be customized to an organization's business model, users, transaction type and volume, and risks. Predictive analytics can identify emerging risks and potential issues that have not yet manifested as incidents.

Payment Systems (and Trust) Are Vulnerable to Financial Crime (Con't.)

- **Build a culture of compliance.** Given that technology innovation can at times outrun controls, some organizations may need to establish a culture commensurate with the financial crime risks they face. Senior leaders can also set a positive tone from the top and promote awareness of financial crime risks across the organization. Training programs and ongoing communication supported by leadership can create and reinforce awareness and compliance.
- **Establish a whistleblower program.** Establishing—or reinvigorating—a whistleblower program can help to reduce internal fraud risk while enabling early detection. A whistleblower program can discourage employees and contractors targeted by external criminals as potential accomplices.
- **Engage with regulators.** Active engagement with regulators can improve all parties' knowledge of PSPs and trends in services, technologies, usage, and priorities.

2022 APG Yearly Typologies Report

Author: Asia/Pacific Group (APG) on Money Laundering
Date Published: July 2022 / Accessed on: 17 August 2022
Source (excerpts from): http://www.apgml.org/methods-and-trends/page.aspx?p=8d052c1c-b9b8-45e5-9380-29d5aa129f45

Use of new payment methods/systems

Indonesia

In 2021, the Indonesian Police collaborated with the Indonesian FIU (PPATK) and related authorities to target crimes on illegal information technology-based lending and borrowing services (peer to peer lending).

There are at least 89 cases that have been identified involving 65 suspects, of which four (4) involve foreign nationals. As for several cases of illegal peer to peer lending, including Company A with business names including Vloan and fintech applications available in the marketplace, including Supercash, Rupiah Cash, Super Funds, Plus Loans, Super Wallets and Super Loans.

Company A is not based in Indonesia and the location of the Vloan application server is located in Country A with hosting servers in Country B. Company A used payment gateway services to send loan funds to customers. If in the process of 7 to 14 working days the service user returns the loan, Company A, through the payment gateway, provides a Virtual Account number from each bank account in the name of Company A.

In addition, there were also cases of illegal peer to peer lending involving Company B. The Indonesian Police have identified 13 suspects with details of seven suspects acting as debt collectors, four (4) suspects consisting of two (2) foreigners and two (2) Indonesian citizens who are directors of Company B. One foreigner is the owner of the Joint-Owned Innovation Savings and Loan Cooperative which has an illegal peer to peer lending service application and another person registered a sim card illegally. The Indonesian Police have blocked and confiscated an account belonging to Company B which was used as a repository for funds with a nominal amount of IDR 239 billion (approx. USD 16 million).

Hong Kong, China

In mid-2021, Hong Kong Police identified an organized crime group engaging in illegal gambling and drug trafficking activities. An operation mounted against the organization resulted in the arrest of 317 persons and the seizure of HKD 735,000 (approx. USD 93,672) in cash in late 2021. A parallel financial investigation revealed that at least HKD 1.35M (approx. USD 172,055) of drugs proceeds were laundered through bank accounts, stored value facilities and the Faster Payment System (a payment financial infrastructure enabling payments across different banks and stored-value facilities on a 24/7 basis introduced in 2018) by the drug traffickers. An investigation is ongoing.

Japan

CEO A of V company and individual B of an affiliated company scammed an individual by informing them that the individual's membership fee for an e-commerce site was unpaid and instructing the individual to pay 50 thousand yen (approx. USD 384) by purchasing pre-paid cards and informing them of the card numbers. After obtaining the card numbers from the individual, they resold the numbers. They concealed the proceeds obtained by the illicit resales, approximately 37 thousand yen (approx. USD 284), in B's bank account. Finally, they were arrested on the charge of the violation of the Act on Punishment of Organized Crime and Control of Crime Proceeds (Concealment of Criminal Proceeds etc.).

Singapore

This case involves the misuse of payment service providers, more specifically via virtual accounts. Virtual accounts are typically offered by banks to their selected corporate clients, such as payment service providers, to allow for the easier identification of their various payers and the purpose of payments for reconciliation purposes.

A Singapore victim of a business email compromise fraud scheme was persuaded into transferring funds to a virtual account maintained by a Singapore bank. Investigations revealed that the Singapore bank had offered virtual account services to a payment service provider operating in Country Y. In turn, the payment service provider operating in Country Y assigned virtual accounts to its clients. The virtual account was later traced to an individual based in Country X. The proceeds were successfully intercepted and efforts are underway to ensure the return of the funds to the victim.

2022 APG Yearly Typologies Report (Con't.)

Use of virtual assets (cryptocurrencies or other virtual assets)

Use of credit cards, cheques, promissory notes etc.

Philippines

Several online news articles and stories circulated in social media regarding several accounts hacked by unknown perpetrators. Based on the report submitted by a bank (which was shared by a Supervising Agency), certain accounts were identified as recipients of the funds from another bank (alleged hacked accounts). Most of the identified recipients had financial transactions, particularly inter-account transfers (outflows), during the period when the alleged hacking incident transpired.

The aforementioned funds which may possibly represent the funds that were unlawfully transferred from multiple accounts were then transferred by the subjects to another bank's accounts (layering), which may indicate that the accountholders may likely be money mules and that their accounts may have been used as a pass-through account. Furthermore, the second beneficiaries, who are either individuals or businesses, appear to be engaged in cryptocurrency trading based on their financial activities.

STRs related to the subjects indicated that their accounts were involved in phishing activities or had received unauthorized fund transfers. The initial beneficiaries had outgoing transactions (inter-account transfers) involving significant amounts which were transacted after the period of the alleged hacking incident. The total amount of debit transactions of some of the subjects almost totalled the amount of their credit transactions, indicating that their accounts were merely just pass-through accounts. According to an online news article, the hacked funds were used to buy cryptocurrencies. During the layering stage, the initial beneficiaries (possible money mules) transferred funds to businesses and individuals (second beneficiaries), some of which were allegedly engaged in cryptocurrency trading. Some of the second beneficiaries have had outgoing transactions to companies who are associated with cryptocurrency exchanges. The second beneficiaries received significant amounts of incoming fund transfers from numerous individuals, which appeared not to be commensurate with their declared businesses and financial capacities.

Subject VA was being investigated for potential violation of R.A. No. 3019 or the Anti-Graft and Corrupt Practices Act. Between 29 October 2004 and 12 January 2021, VA figured in 314 covered transactions and four (4) suspicious transactions ranging from PHP 39,227 (approx. USD 741) to PHP 15 million (approx. USD 283,504) and totalling PHP 410.439 million (approx. USD 7,757,420).

One (1) suspicious transaction pertained to a purchase of a life insurance policy in cash by VA's son in August 2020. The named beneficiaries in the insurance policy were the wife, daughter, and another son of VA. **The three (3) remaining suspicious transactions pertain to unauthorized credit card purchases** totalling PHP 168,326 (approx. USD 3,181) made in VA's account in May 2019.

In addition to these, VA was also found to have various large investments in different high- yielding products with three domestic banks, which are likely methods to launder the proceeds of unlawful activities, particularly for graft and corruption.

It is noteworthy to mention that **VA made three (3) large credit card purchases ranging from PHP 500 thousand (approx. USD 9,450) to PHP 1 million (approx. USD 18,900) in 2019**. There were also large transfers of funds, through cheques between VA and his presumed relatives.

Based on the reports on salaries and allowances of a domestic government agency, VA's average monthly salary in prior years was less than PHP 100 thousand (approx. USD 1,890). After being promoted in 2016 to his current position, VA's average monthly salary ranged between PHP 187 thousand (approx. USD 3,534) and PHP 240 thousand (approx. USD 4,536). The compensations of VA are significantly lower compared with his reported transactions from 2004 to 2021; hence, VA's transactions are perceived not commensurate with his known source of income (his salary) and financial capacity.

Hongkong Money Laundering and Terrorism Financing Risk Assessment Report

Author: Financial Services and the Treasury Bureau
Date Published: July 2022 / Accessed on: 27 July 2022
Source (excerpts from): https://www.fstb.gov.hk/fsb/aml/en/doc/2nd%20HK%20ML%20TF%20Risk%20Assessment%20Report_e.pdf

SECTORAL RISK ASSESSMENT – FINANCIAL INSTITUTIONS
ML Vulnerabilities of the Banking Sector: Payment systems and new payment methods (NPM)

NPM providers have emerged and gained popularity globally, including in Hong Kong. While NPM providers often provide genuine economic benefits by offering faster and more efficient payments at lower cost, they generally utilize bank accounts to conduct payment transactions on behalf of their customers and may increase ML/TF risk by inserting additional intermediaries into payment chains, making it harder to "see through" to the originator and final beneficiary. As NPM providers mainly operate through online platforms, it may be difficult for the "host jurisdiction" to confirm their principal place of business due to their transnational nature and dynamic business models. Given their easy accessibility and sometimes unclear regulatory status, NPMs may become attractive to criminals for ML/TF, which poses challenges to banks in assessing and mitigating risks. There has been little evidence that abuse of NPMs for illicit purposes is prevalent in Hong Kong, although the use of some NPMs, including the use of VAs, was observed in some ML cases. Banks have become increasingly aware of the ML risks posed by NPMs and have conducted reviews where appropriate to identify and assess their exposure to threats arising from NPMs and understand fund flows of accounts that potentially use NPMs for ML/TF purposes. Some banks have already implemented or amended controls (e.g., targeted CDD measures) to address any identified risks. Donation-based or crowdfunding platforms, often operating in conjunction with NPM providers, are another development that may present risks, including for TF and other illegal activities.