OliverWyman

COMBATING DIGITAL-ERA MONEY LAUNDERING AND TERRORISM FINANCING

Perspectives on digital payments and payment service providers

Rod Francis
Lilian He
Jacky Tam

EXECUTIVE SUMMARY

As digital payment volumes and penetration rates continue to grow fast, digital payment service providers (PSPs) have become important players in the global financial ecosystem. However, this sector is still considered to be a weak link in combating money laundering and terrorist financing.

Digital PSPs face multi-fold challenges. On the one hand, they often have to deal with a more fragmented regulatory landscape compared to traditional financial institutions (FIs), such as banks, for which regulators impose different licensing and regulatory oversight requirements. As a result, digital PSPs are more vulnerable targets for criminals who have the capabilities to exploit this "regulatory arbitrage". On the other hand, compared to the business models of traditional FIs, the digital payment and banking model presents unique risks and challenges that require further attention. These include the following: the rising resource and customer experience challenge to handle high-volume, short-turnaround-time transaction monitoring; the increasing challenge to detect and combat digitally savvy "money mules"; the evolving "merchant risks" associated with ecommerce payments; AML/CFT compliancy in the "white labeling" business model; and the risks associated with cryptocurrency-related payment transactions.

In response, regulators globally have collectively stepped up their scrutiny of the money laundering and terrorism financing risks of PSPs with various actions. These have added pressure not only to digital PSPs in terms of their financial and reputational risks, but also to players in the broader financial ecosystem, such as banks, which facilitate such payment transactions and so may need to de-risk by no longer working together with any non-compliant or high-risk players in the payment sector. Therefore, it is essential for digital PSPs to take action now to address their AML/CFT challenges.

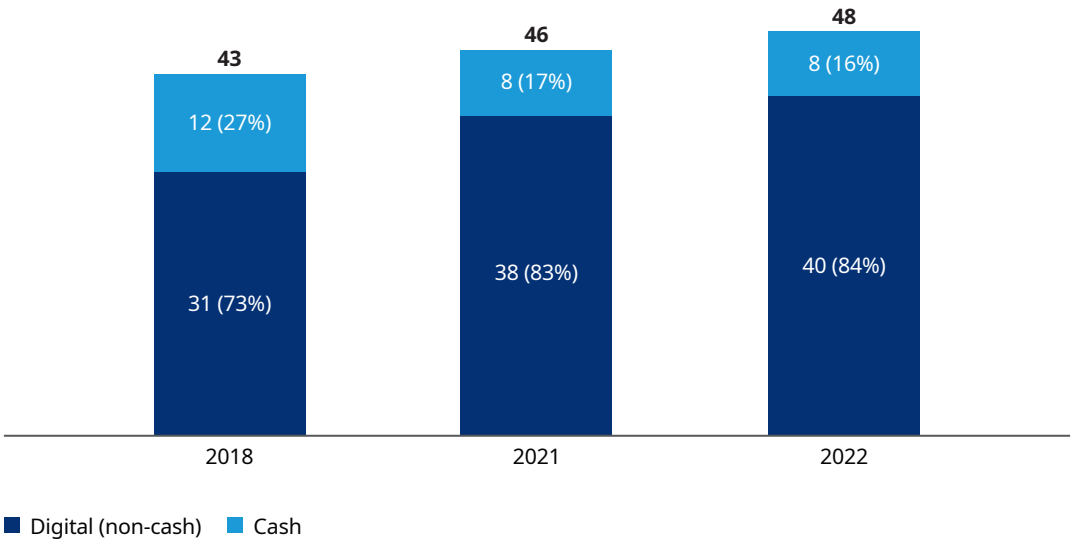
As financial services firms' business models and ways of serving customers have evolved toward a digital landscape, risk management and compliance should not be left behind. Leveraging data and technology better to address the existing and emerging risks will be critical in order to enable a digital proposition in a risk-robust, compliant, and scalable way. We believe that PSPs and broader digital players should consider three building blocks in particular, namely, transforming from a rules-based to a risk-based approach by leveraging advanced analytics on transaction monitoring and dynamic customer-risk assessment; automating at scale to manage costs and improve overall workflow efficiency; and embedding AML/CFT controls in their design as an integral part of defining a seamless digital journey for customers.

While the above enablers are critical and innovative ways to address the emerging challenges, it is important to start by understanding the risks and getting the basics right. Raising the overall AML/CFT capabilities of digital players is a journey in the right direction, and Oliver Wyman is here to help.

STRONG PAYMENT GROWTH BUT PERSISTENT RISKS

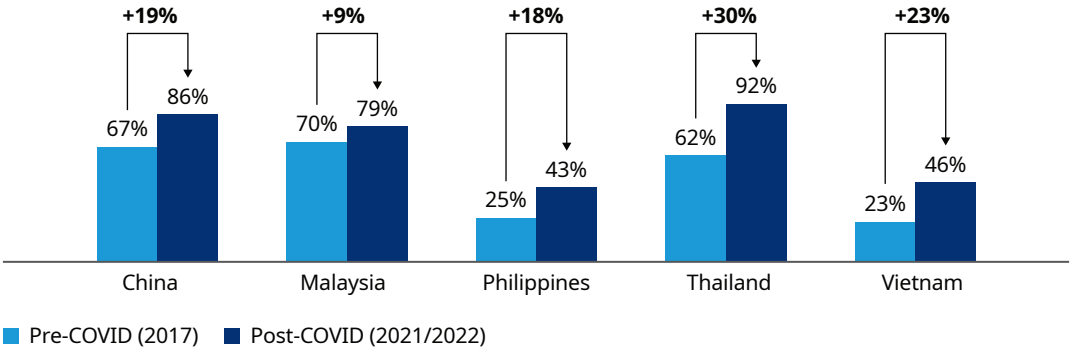
The pandemic has accelerated the growth of digital payments in significant ways. Digital payments now account for 84% of transaction value globally (see Exhibit 1). Digital payments continue to surge, particularly among major markets in the Asia-Pacific (APAC) region and penetration has reached new heights. According to the World Bank, China already has an 86% penetration rate for digital payments, defined as including digital transfers to and/or from banks, other financial institutions, or with a mobile money provider, up from 67% before the COVID-19 pandemic. Other markets such as Thailand and Vietnam have experienced a surge in adoption by about 20% to 30% from 2017 to 2021 and 2022, respectively. This kind of growth should remain sustainable with the passing of more financial inclusion policies, and more payment technologies, such as quick response (QR) codes and buy now, pay later (BNPL) functionalities, emerging and becoming available (see Exhibit 2).

Exhibit 1: Global payment transaction value, 2018 to 2022
In US $ trillion



Source: Worldpay global payments report 2023

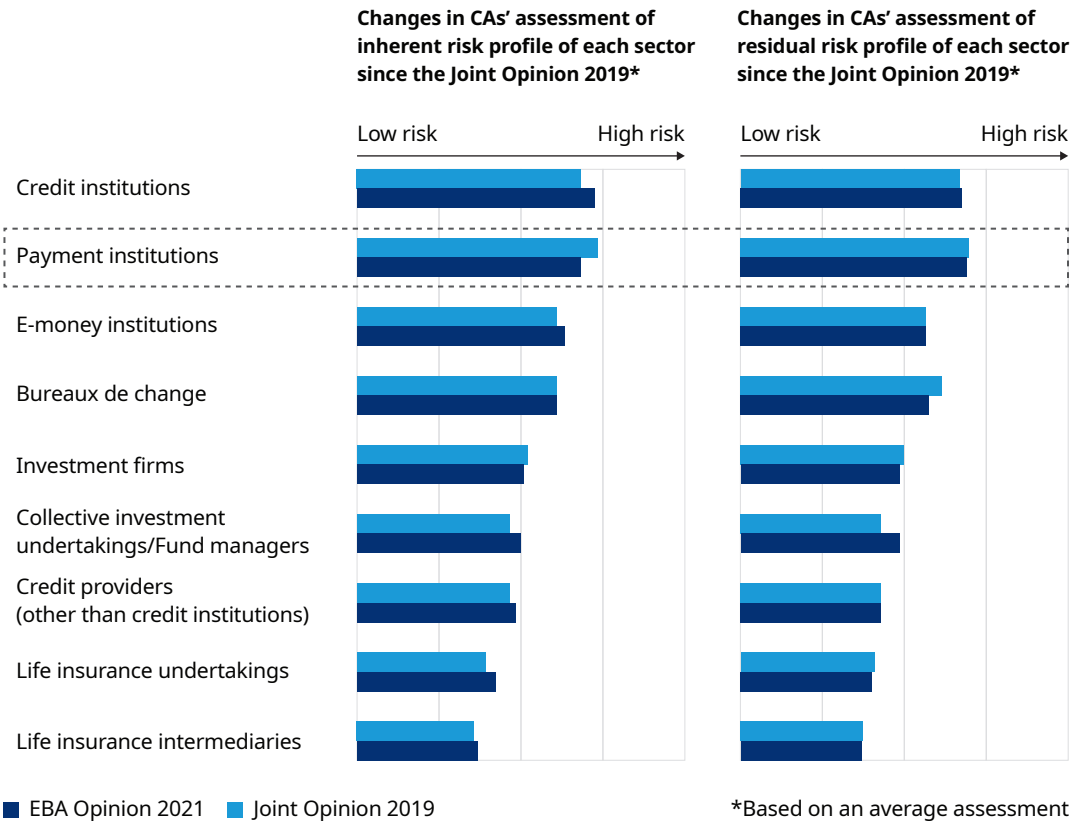
Exhibit 2: Digital payment penetration of certain APAC markets, 2017 to 2022
Percentage of adult population



Source: World Bank Global Findex Database

With the exciting growth, however, the payment space continues to be a high-risk channel for money laundering and terrorism financing (ML/TF) activities. According to a recent European Banking Authority (EBA) report (see Exhibit 3), regulators continue to see payment and e-money institutions as the riskiest sectors for ML/TF within the financial services realm.

Exhibit 3: EBA's average ratings of ML/TF risk assessment in the financial sector



Source: European Banking Authority

The fragmented regulatory landscape also adds further challenges to mitigating the risks. Varying PSP-licensing requirements, ambiguity on the AML/CFT requirements for PSPs, and differing oversight/enforcement mechanisms make it challenging for cross-border, multi-market, digital PSPs to comply with all the requirements across all the respective jurisdictions. For instance, some markets' AML/CFT regulations do not require PSPs to be reporting entities. Such regulatory gaps not only put PSPs at risk, but also give criminals the chance to exploit them as a form of "regulatory arbitrage" for illicit cross-border transactions.

Regulators across the region have collectively stepped up their scrutiny of PSPs' ML/TF risks with various actions (see Exhibit 4). They are calling out PSPs for material ML/TF concerns. These stories not only make headline news, but PSPs also often have to pay hefty fines in the millions or even billions of dollars, not any less than the fines issued to banks and other financial institutions.

PSPs that are unable to uphold AML/CFT standards also have a higher likelihood of being de-risked by their bank counterparts. This would involve declining PSP's access to financial services or having them exit their existing banking relationships in line with the respective banks' risk appetite. Such actions would put PSPs in a tough position, affecting their business operations, brand reputation, and customers' payment experience.

Exhibit 4: List of AML/CFT regulatory actions

	Key regulatory actions	Descriptions
1	Enhanced regulatory requirements	Regulators have imposed enhanced regulatory requirements on digital PSPs to mitigate money laundering risks. These include "know your customer" (KYC) and AML regulations, and transaction and risk monitoring requirements. Digital PSPs must meet these requirements before receiving legal authorization to operate. Regulators have also mandated licensed PSPs to continuously report and/or comply with AML/CFT standards across Asia-Pacific markets, such as China, Indonesia, Malaysia, the Philippines, Singapore, and Vietnam.
2	International cooperation	Regulators have collaborated internationally to establish common standards for digital remittances and payments. These include regulations such as the Financial Action Task Force guidelines, which establish global AML/CFT standards to regulate digital PSPs.
3	Emerging technologies	Regulators have examined the use of emerging technologies to help reduce the risks of money laundering in the industry. These include blockchain-based solutions, biometric authentication, and artificial intelligence transaction analysis.
4	Enforcement	Regulators have increasingly taken action to ensure that digital PSPs comply with regulatory requirements. These include imposing fines, revoking licenses, and criminally prosecuting non-compliant digital PSPs.

Source: Oliver Wyman analysis

Overall, the implication on PSPs and their facilitating banks is clear: the stakes are much higher for digital PSPs. With their increasing significance in the financial sector ecosystem, and the increasing scrutiny and potentially costly outcomes of non-compliance, there is an urgent need for digital PSPs to raise their AML/CFT controls.

In the following sections, we will further look at the emerging challenges arising from digital business model innovation. These challenges are contributing to rising AML/CFT risks, particularly to digital PSPs, calling for more effective controls and mitigations to adapt.

EMERGING RISKS OF DIGITAL PSPs

Growing volume and scale, the expansion of business and geographical coverage, and the fragmented regulatory landscape are all adding pressure to PSPs, potentially making them more vulnerable to threats and criminal exploitation. Additionally, as payment services, specifically digital ones, become increasingly embedded in the broader financial ecosystem, it is increasingly critical and challenging to ensure the transparency of ML/TF risk management, not only within each respective PSP but also externally with other financial service facilitators in the ecosystem, such as banks.

With the evolvement of the digital PSP business model, we believe that digital PSPs are facing five new risk dynamics and challenges that they will need to address.

The rising resource and customer experience challenge to handle high-volume, short-turnaround-time transaction monitoring

In the digital-first era, epitomized by ecommerce, social commerce, and P2P payments, customers desire a seamless payment experience. PSPs are therefore pushed to deliver a much higher payment volume processed per second, and instant settlement times of seconds rather than one or two working days, for both domestic and cross-border transactions.

Behind this shift lies the challenge of transaction monitoring. The existing rules-based transaction monitoring approach, even with careful calibrations and threshold settings, may still lead to a large volume of alerts due to the sheer volume of transactions, and may also include a high number of false-positive cases. With investigation and response times limited, there is usually added pressure to team resources in order to manage the large backlog of alerted cases.

The challenge therefore requires digital PSPs to take a more risk-based approach to transaction monitoring. Advanced analytics for the prediction and detection of ML/TF patterns with a high level of precision would provide PSPs with a strong toolkit to prioritize and allocate resources to cases that require the transaction monitoring team's further investigation. At the same time, it would help reduce the number of interrupted transactions that would negatively affect the customers' payment experience.

The increasing challenge to detect and combat digitally savvy "money mules"

Detecting money mules in the digital sphere is more challenging for digital PSPs than it is for banks to detect traditional money mules who utilize bank accounts. This is because criminals and money mule recruits who target digital PSPs are often digital natives. As highlighted in recent money mule cases in Asia, many of these individuals gathered sufficient intelligence and experience by experimenting with the onboarding processes, transfer limits, and other parameters of various digital payment platforms. By doing so, they learned how to exploit the procedural differences or loopholes from the more vulnerable PSPs. In some cases, they were even able to bypass the usual onboarding controls and rules-based activity monitoring.

The evolving "merchant risks" associated with ecommerce payments

The rising prominence of ecommerce has complicated the conventional approach to AML/CFT in two major ways. The first is the on-screening for any merchant risks. This refers to the validity of the business or merchant accounts on the various payment platforms and their risk of being a front or shell entity for illicit transactions. This is particularly alarming in the scenario where a digital wallet is embedded as part of the ecommerce platform's merchant offerings, such that the opening of the wallet account is a "straight-through" process without any additional AML/CFT due diligence by the PSPs. Unsavory individuals could easily get high-risk accounts onboarded via such a convenient channel, and they could remain unvalidated on the books unless the PSPs have ongoing monitoring and review protocols in place.

The other concern is to do with the detection accuracy of questionable transaction patterns. Many conventional ML/TF typologies, such as high-frequency or single, large-size transactions, are now commonly seen for legitimate ecommerce purposes, such as group purchases. They also introduce an element of ambiguity for truly suspicious transactions, as the perpetrators of these can disguise or blend them into other acceptable payments in terms of their payment structure and declared purpose of transaction. Therefore, most PSPs could lack sufficient granular data points and data analytics techniques, such as peer-anomaly detection based on the types of merchants or transactions, to pinpoint true-positive cases of ML/TF among the rest.

AML/CFT compliancy in the "white labeling" business model

PSPs are offering an emerging business model of "white labeling" to their non-payment partners, such as retail conglomerates and leading consumer applications, leveraging their payment infrastructure and licenses without establishing direct customer relationships with the end-users.

Digital PSPs should not overlook any misalignment of AML/CFT controls with their white-labeling partners. While PSPs may wish to rely on these partner institutions for their customer due diligence and AML/CFT controls, particularly since the institutions own the customer-facing relationships and interface, such players may not be established financial institutions, and hence may lack the capabilities and knowledge to deliver the required assurances.

Additionally, any barriers to data sharing or collaboration between the partners could hinder appropriate AML/CFT mitigation, such as insufficient data disclosure, or reporting delays between the partners.

The risks associated with cryptocurrency-related payment transactions

Some PSPs allow the use of cryptocurrencies to facilitate money transfers. Senders and receivers can use cryptocurrencies to conceal their real-world identities and locations, significantly increasing the difficulty of AML/CFT detection, and magnifying the risk of any known onboarding control gaps of the PSPs and/or their partners responsible for the cryptocurrency transactions. Moreover, the differences in the regulators' pace in addressing these issues from one market to the next would be another grey area for "regulatory arbitrage", particularly affecting PSPs that facilitate fiat-to-cryptocurrency transactions today.

These challenges require digital PSPs to re-assess the applicability and effectiveness of a conventional approach to AML/CFT controls in comparison to a more analytics-driven approach. Digital PSPs also need to take a more integrated approach to consider the implications to their business model and their customers when embedding such controls.

FUTURE-PROOF ENABLERS FOR DIGITAL PSPs

As financial services firms' business models and ways of serving customers have evolved toward a digital landscape, risk management and compliance should not be left behind. Leveraging data and technology better to address the existing and emerging risks will be critical to enable digital PSPs, banks, and other financial institutions to deliver their digital propositions to customers in a risk-robust, compliant, and scalable way.

We believe that digital PSPs should consider the following building blocks to help uplift and future-proof their capabilities. These principles and considerations are also applicable to the broader digital banking communities that aim to deliver successful digital propositions and customer journeys.

Rules-based to risk-based, analytics-enabled monitoring approach

Digital PSPs can leverage advanced analytics, such as machine learning, to shift from a rules-based to a risk-based view on transaction monitoring. Doing so would help optimize the PSPs' resource allocation to high-risk cases, while also minimizing the volume of false-positive cases. At Oliver Wyman, we support our clients in implementing advanced analytics with use cases in transaction monitoring and customer risk reviews.

One example is machine learning-based behavioral analysis and anomaly detection in transaction monitoring. This type of analysis identifies financial crime patterns beyond simple rules-based alerts. Rather, it creates triage-level alerts based on risk levels so as to enable better prioritization and action decisioning.

Another example is dynamic customer risk assessment analytics to adjust the risk score of individual customers by considering a combination of historical and real-time transactional behavior, external data verification, and existing rules-based alerts. Such analytics help digital PSPs to move away from the periodic review model to a more risk-triggered model for customer due diligence and reviews.

Lastly, network analysis involves leveraging large volumes of payment flows and accounts' data to identify clusters of linked parties within the digital PSP's customer base, providing stronger traceability and depth into the suspicious payment activities being flagged. Doing this allows for a holistic and dynamic review of interconnected parties and transactions, breaking away from siloed investigations

Automation at scale

Digital PSPs can automate at scale to manage their costs and uplift their efficiency. The sheer volume and scale of digital operations make traditional, manual-based controls and testing less applicable to digital PSPs. Digital PSPs therefore need to think through their end-to-end workflow automation and case management flow, including exploring digital solutions on "know your customer" (KYC) and risk assessments, and data extraction and ingestion to quickly aggregate disparate information sources together so as to supplement post-scenario analytics and investigations.

Control by design

Digital PSPs can control by design by embedding AML/CFT checks in their digital customer experience design. To deliver their value proposition and digital customer journey, digital PSPs, as well as broader digital banks, need to consider AML/CFT controls as an integral part of their customer experience design. For example, digital PSPs should consider the sequence of the controls to optimize the journey's drop outs and lead times, the approach on data capturing, such as deriving or extracting instead of asking for input from customers, and leveraging external data sources to cross-reference digital customer touchpoints.

While the above enablers are critical and innovative ways to address the emerging challenges, it is important to start the whole uplift journey with a comprehensive assessment of risk. Only by doing so can digital PSPs properly understand where their challenges lie and the specific regulatory expectations they need to meet, so that they can truly get the basics right and address any existing gaps in their controls.

Raising the overall AML/CFT capabilities of digital players is a journey in the right direction, and Oliver Wyman is here to help.

Oliver Wyman is a global leader in management consulting. With offices in more than 70 cities across 30 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 6,000 professionals around the world who work with clients to optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities.

For more information, please contact the marketing department by phone at one of the following locations:

Americas	Europe	Asia Pacific	India, Middle East & Africa
+1 212 541 8100	+44 20 7333 8333	+65 6510 9700	+971 (0) 4 425 7000

AUTHORS

Rod Francis
Partner
rod.francis@oliverwyman.com

Lilian He
Principal
lilian.he@oliverwyman.com

Jacky Tam
Engagement Manager
jacky.tam@oliverwyman.com