INSTITUTE of INTERNATIONAL FINANCE

Payments Security and Trust

IIF Staff Paper
September 29, 2023

Executive Summary

We are at an inflection point in the global payments agenda. While the official sector has set out challenging targets for cost, speed, and transparency in cross-border payments, there are emerging threats to trust and security that demand significant resources and industry focus at a time when they could be curtailed by changing market conditions and the policy focus on other metrics.

- A recent survey of SMEs and consumers found that security was the most important factor when choosing a cross border payment provider
- Global spending on information security and risk management is forecast to grow 11% annually to $267.3 billion by 2026
- Payment service providers will need to see a positive business case for continued investment in payments security

New challenges include:

- Generative AI enhanced fraud – the dramatic increase in plausibility of phishing and deepfake scams directed at payments users trick people into revealing sensitive information, sending money or buying fake products
- Greater complexity of the payments ecosystem – financial institutions and paytechs see and react to greater demand for embedded payments and complex partnerships with tech platforms across multiple dimensions
- Sanctions screening requirements within cross-border payments continue to grow in volume and complexity of implementation

This paper highlights the role of trust and security in payments, explores various challenges, examines how financial institutions and paytechs are addressing them, and lays out some opportunities for public-private collaboration.

1 The primacy of trust and security in payments

Security and trust are essential success factors for the adoption of digital payments, especially in cross-border transactions where different regulations, currencies, and risks are involved. Without security and trust, low-cost, faster, or more transparent payments are of diminished value.

Indeed, security is one of the three foundational attributes of payments, alongside integrity/failure rate and resilience. Speed (of clearing, settlement, funds availability), transparency and predictability of fees and timing are seen as among the differentiators. Importantly, different users may value different dimensions of payments, and may trade off speed, cost, and transparency in different ways according to use case. A December 2022 survey by SWIFT of consumers and small businesses in Australia, China, Germany, India, Saudi Arabia, South Africa, the UK, and the US found that security was the most important factor, for both consumers and businesses, when choosing a payment provider to send money across borders.

Faster payments may make certain types of fraud, such as authorized push payment (**APP**) fraud, easier and potentially more devastating. As frictions in payments are reduced, the scope for bad actors to access substantial consumer banking, investment or pension balances is increased and the ability for intermediaries to block transfers is decreased. As faster payments systems start to be linked internationally, sanctions screening and other risk management requirements become a greater imperative as well. One in every five global consumers fell victim to payments fraud in the last four years. 27% of these victims were the subject of an APP scam.

The payments ecosystem is becoming more complex and the compliance and user experience environment more demanding. New paytech entrants are fueled by significant funding activity; total global investment (measured across VC, PE, and M&A) in new payments technology grew strongly in 2021 and 2022, totaling $57 billion in 2021 and $56 billion in 2022 globally, well up from $30 billion in 2020. KPMG anticipates an increasing focus by payments providers on B2B payments in H2 2023, particularly the use of real-time payments, as businesses look to optimize their supply chains, automate processes, and improve their anti-fraud efforts.

1.1 Level of investment needed to meet the growing challenge

Maintaining security and trust in payments requires an ever-increasing commitment from financial institutions and paytechs as they confront growing risks and constant change in technology.

Fighting crime is expensive, time- and labor-intensive work. Over the past five years, one card scheme has spent more than $10 billion on technology, including to reduce fraud and increase network security. 85% of surveyed small and midsize enterprises (which include many fintechs and payment companies) intended to increase IT security spending into 2023.

Globally, research firm Gartner predicts that global spending on information security and risk management will grow to $188 billion in 2023 and by 11% annually to $267.3 billion by 2026. Over 21% compound annual growth is forecast for direct cyber insurance premiums until 2025, showing increased demand to insure against cyber risks.

There is an emerging talent shortage in this critical field for payment security: there are reportedly 3.5 million open cybersecurity positions worldwide. Whether some or many of these positions will ultimately be filled by AI-enhanced algorithms, remains to be seen.

Payment fraud is expected to continue increasing and is projected to cost $40.62 billion globally in 2027. Payment fraud cases and skimming attacks spiked 164-174% from mid-2021 to mid-2022. The cost of digital crime more broadly is projected to reach $10.5 trillion annually by 2025, up from $3 trillion in 2015.

Not surprisingly, cybersecurity was viewed as a top year-ahead risk according to the 12th Annual EY-IIF Global Bank Risk Management Survey of banking CROs from 88 financial institutions across 30 countries. Similarly, digital security and crime was seen as a top 10 risk by over 1,200 experts and 12,000 business leaders in 121 economies over both the short and medium term, with links to other risks such as misinformation/disinformation, and breakdown of critical information infrastructure.

An MIT Technology Review survey found payments, data and systems security threats to be the biggest challenge (59%). 42% of respondents said security measures are important to their customers and adopting more advanced security capabilities, including enhanced authorization technology like tokens (32%) and fraud detection through biometric authentication and AI (43%), is a priority for many.

The ability for the private sector to continue allocating capital to these efforts requires a positive outlook on the business case for payments. Long term investment commitments to the development of next generation technology for payments security fuels an ecosystem of ventures, entrepreneurs, and technology firms the world relies on to maintain security and trust.

2 Emerging challenges to trust and security in payments

Three particular challenges are emerging to established paradigms in payments security, from different directions.

- **Generative AI**, particularly the dramatic increase in plausibility of phishing and deepfake scams directed at payments users
- **Greater complexity of the payments ecosystem**, as financial institutions and paytechs see and react to greater demand for embedded payments and complex partnerships with tech platforms across multiple dimensions
- Increasing focus on enforcing **new regulations and sanctions** within cross-border payments as they continue to grow in volume

2.1 The challenge from AI-enhanced frauds and scams

AI-generated and AI-designed scams and fraud are on the rise, posing a serious threat to consumers, financial institutions, and fintechs. Criminals are using advanced AI technologies

such as voice cloning, phishing, and chatbots to trick people into revealing sensitive information, sending money or buying fake products. These scams are increasingly difficult to detect and prevent, as AI can process large amounts of data, perform tasks quickly, evade detection, and create convincing fake or misleading information.

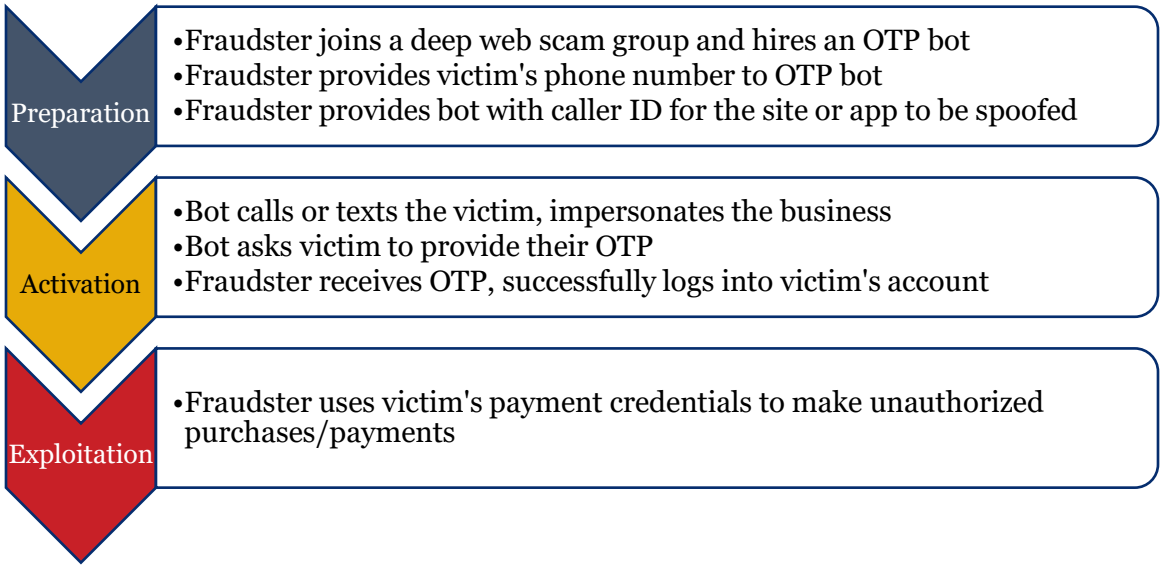
In 2023, the new category of generative AI burst to prominence. These systems permit users to generate completely new content with a few prompts, including text, synthetic photographs, and cloned voices. While promising great productivity benefits, this type of AI also hands fraudsters and other bad actors powerful tools for creating fake, but compelling, content that can be much harder to spot than previous efforts.

One of the most alarming examples of AI-enabled fraud can be voice cloning, which involves using AI tools to recreate a person's voice after listening to them speak for a few seconds. This technology can be used to create fake voicemails or messages, for instance to imitate family members requesting payment of ransom money or to clone the voice of a company director to steal $35 million. One reporter used this technology to reportedly gain access to a bank account with an AI-replicated version of his own voice. Another journalist was able to self-clone his voice to gain access to his government benefits self-service account. Voice command features are now also being added to payment systems such as UPI in India in an effort to overcome illiteracy and drive inclusion. Careful consideration of the risk, or added authentication and security features, will be needed to avoid creating a new pathway for fraud.

Generative AI can also make authorized push payment (APP) scams easier to design and deploy. Previously reliable clues to phishing emails or SMSs such as bad spelling or grammar are no longer present, for example. In the six months since ChatGPT launched for public use in November 2022, nearly half of consumers in one survey admitted to finding it more difficult to identify scams, although perhaps surprisingly 80% still felt confident they could spot AI-generated content. And another 78% of consumers expressed concern about AI being used to defraud them.

Social engineering strategies can be quickly developed or deployed using large language models that have had the guardrails deliberately removed, such as FraudGPT. Phishing kits and "phishing-as-a-service platforms" are now available on the dark web, where criminals can access pre-built phishing templates, tools, and resources. AI has become the latest tool to increase the volume and sophistication of phishing attacks. Automated one-time password (OTP) scams are one type of fraud enabled by phishing-as-a-service (see **figure 1**).

Figure 1: Stages of an automated OTP scam



Source: IIF staff, adapted from Sift, Fighting fraud in the age of AI and automation

2.2 Ecosystem complexity

The banking and payments ecosystem is undergoing a rapid transformation, driven by new technologies, business models, participants, and forms of money.

The digital transformation of financial services extends activities—such as embedded payments, stored value, and receivables credit—into broad and complex ecosystems, with many new players and shifting roles. These ecosystems are evolving with dynamic value networks of diverse actors who create value through complex models of collaboration, competition, and innovation.

This transformation brings new opportunities for convenience, efficiency, and inclusion, but also new security challenges that need to be addressed to ensure the safety and trust of the system.

Open finance (and open banking) is a policy trend accelerating these changes in payments. Open finance takes the form of a framework or regulation or voluntary incentives that allow consumers to access and share their financial data with third-party providers, such as fintech apps, payment services, or lenders. Open banking refers to data from institutions with banking licenses, while open finance can enable the consumer to share access to their broader financial footprint. The same level of security precautions are not always provided by the different entities accessing this sensitive data along the chain.

Security challenges from the increasing complexity of the payments ecosystem include:

- adapting web application firewalls for enhanced user experience and service networking as traditional web apps become outdated

- protecting application programming interfaces (APIs) from attacks and breaches, given their central role in data exchange and service integration in open banking

- managing API access with authentication, authorization, consent, and revocation to allow only legitimate third-party access

- misuse of data beyond consumer's consent by third parties that have legitimate access to it

As ecosystems become more complex and contracting chains longer, third party operational risk management becomes a topic of focus, a topic on which we recently wrote to the Financial Stability Board.

Open banking and finance present challenges beyond the specific issues in focus in this paper, by reshaping roles, responsibilities, and economic models in the financial ecosystem. The impacts of these developments alongside new data policies evidence the importance of broadening the regulatory scope of these initiatives from open finance to open data.

2.3 Geopolitics and sanctions screening

While the armed conflict in Ukraine has thrown into sharp relief the importance of sanctions screening in payments, the need for financial institutions and paytechs to keep track of an ever-growing list of individuals, entities, and blockchain addresses subject to sanctions by one or more jurisdictions is not new.

Sanctions screening is becoming more challenging for financial institutions due to the increasing complexity and diversity of sanctions regimes, the growing volume and speed of cross-border payments, and heightened user experience (UX) expectations. Sanctions screening can of course impact UX, as false positive alerts may cause delays or rejections of payments, abandoned transactions, and even brand damage. Difficult choices and trade-offs are faced by internationally active FIs and paytechs, including from conflicting laws between jurisdictions.

Given the stakes, reducing false positive and false negative rates are both crucial. Individual name matching is a "hard nut to crack" both in AML and sanctions screening:

> *While Fuzzy Algorithms can help with some of the real-world challenges like typos, incomplete strings, etc. some issues like transliteration issues, nicknames, spelling differences can't be mitigated with any fuzzy algorithm. The results are either an overload of false positives or, even worse, false negatives. – sanctions.io*

Many respondents to a 2021 survey by the Financial Action Task Force (FATF) highlighted sanctions screening and transaction monitoring as one of the most significant cost elements where there are widely differing requirements, expectations, and complexity between different jurisdictions.

Sanctions screening is particularly challenging for real-time payments, which require fast and accurate screening of data within domestic transfers. Incumbent payment screening infrastructure may not be able to cope with the volume and speed of real-time payments,

particularly as domestic faster payment systems are connected internationally. For major European banks, nearly half (47%) of sanctions alerts were reported in 2019 to take longer than a day to process, with almost 100% processed after 5 days.

Some of the key challenges around sanctions screening processes include:

- frequently updated sanctions lists and changing customer KYC profiles
- sanctions are complex, varying in scope, target, and duration, while restricted parties use advanced evasion tactics
- naming inconsistencies pose a risk to accurate screening, especially for foreign entities

A lack of data models and standards, particularly relating to unilateral sanctions, and the fact that some sanctions lists are still published in PDF format requiring data extraction, and/or do not use global identifier schemes such as the legal entity identifier (LEI) or branch identifier code (BIC), add additional challenges. An analyst requires 30-45 minutes on average to investigate an Alert/Case according to a Tata study. The majority of this time is typically consumed by gathering information from various external and internal sources.

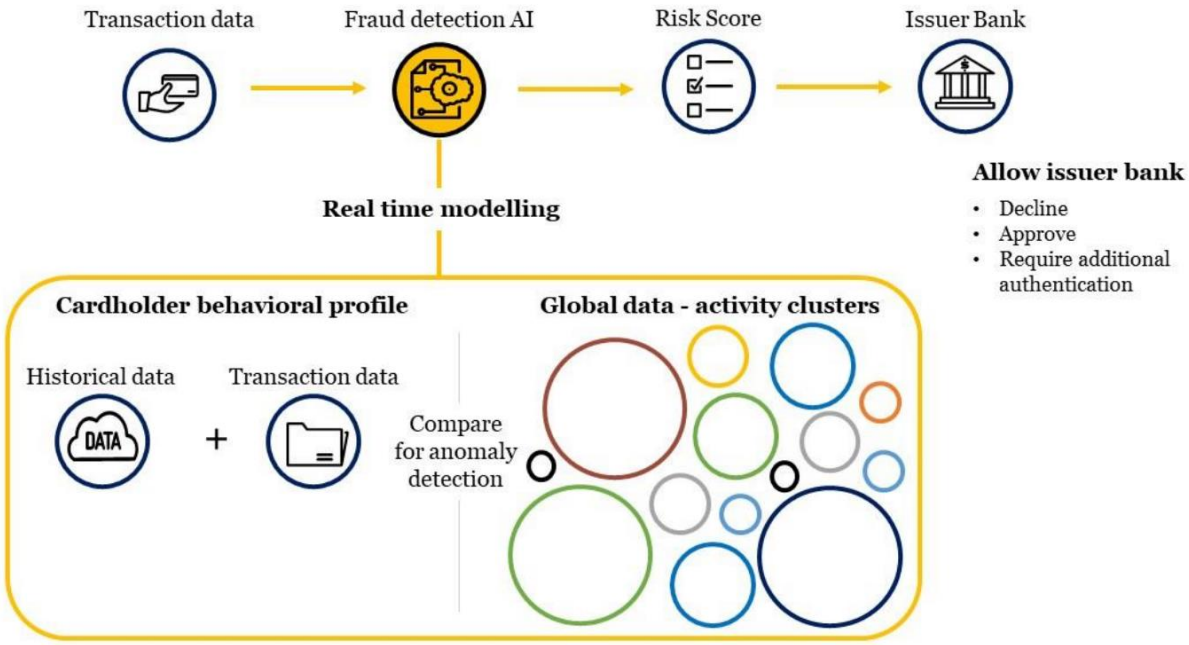
3 How financial institutions and paytechs are addressing the challenges

3.1 Fighting fraud with advanced detection and prevention

The panorama of financial fraud is vast and ever-changing, with concerns running the gamut from identity theft to refund abuse. Card testing and first-party misuse—such as fraudulent chargebacks—are prevalent, but the rise of APP fraud has recently emerged as a pressing issue in multiple jurisdictions. This diversification of fraud types calls for robust, adaptable, and real-time prevention and monitoring solutions deploying AI and machine learning.

Real-time fraud detection models are increasingly driven by AI and machine learning to detect anomalous transactions (see **figure 2**). As we highlighted in our January 2023 report, the use of AI and machine learning is proving to be a game-changer in the fight against financial fraud. With unsupervised machine learning, these technologies require more data to train but fewer human resources to operate. Their true strength lies in their ability to unearth previously unknown patterns of fraud, offering a more comprehensive and proactive approach to security.

Figure 2: AI-drive real-time fraud detection



Source: IIF, Data Policy Impacts - Fraud Prevention (January 2023)

At the same time, banks, consumers and fintechs need to be aware of the potential risks of AI-enhanced fraud and take appropriate measures to protect themselves. Some of the possible solutions include:

- implementing AI-based fraud detection and prevention systems that can analyze data and identify patterns that may indicate fraudulent activity, including deepfake and other synthetic content
- educating customers and employees about the signs of AI fraud and how to avoid falling victim to it
- collaborating with other stakeholders such as regulators, law enforcement agencies, and industry associations to share information and best practices on combating AI fraud

Fraud prevention/monitoring via AI and machine learning

Role of Third-Party Service Providers: In this high-stakes game of fraud prevention, innovative new third-party service providers play a crucial role, offering a multilayered security architecture that is flexible across various sectors and geographies. Emerging solutions use AI and machine learning techniques to tackle financial fraud, from detecting sophisticated scams through behavior biometrics to analyzing large data sets for proactive fraud identification.

Preventing "friendly fraud": Some solutions offer post-purchase anti-fraud measures, aiming to minimize the impact of chargeback fraud, often referred to as "friendly fraud" or "first-person fraud". Their services go beyond detection and offer comprehensive solutions that aid in dispute resolution, providing a one-stop-shop for merchants and financial institutions alike.

Advancing payment security through tokenization: While tokenization of Personal Account Numbers (PANs) has been a standard practice for some time, the industry is now witnessing the rise of so-called "network tokens." They not only replace sensitive information with a unique digital identifier but also integrate more dynamically with payment networks, facilitating higher authorization rates, significantly lower fraud levels, and an overall enhanced customer experience.

Deepfakes and bot detection: New players are emerging to help financial institutions "fight fire with fire" – such as by helping to detect fake identity documentation, often itself generated by AI.

Evolving rules and support systems: Given the dynamic nature of fraud, the rules surrounding compelling evidence and dispute resolution are continually being updated. Paytech platforms are incorporating these changes into their compliance and governance models, ensuring that they remain aligned with the latest legal frameworks.

By leveraging cutting-edge technologies and partnering with specialized third-party service providers, the financial industry is making significant strides in real-time fraud prevention and monitoring. As we navigate this complex landscape, the evolving governance models and regulatory frameworks will serve as the lynchpins that hold these advanced systems together, ensuring a more secure and trustworthy financial environment for all stakeholders.

3.2 Addressing the ecosystem challenge with improved trust and identity services

Adopting a risk-based approach to security involves identifying, assessing, prioritizing, mitigating, and monitoring the security risks in the new, more complex payments ecosystem, including in those jurisdictions with regulatory or market-led open banking ecosystems.

Multiple strategies (**see box**) are being deployed to address the challenges from a security and risk management perspective of the growing complexity of the payments ecosystem, including in the open banking context:

- adopting advanced digital trust solutions leveraging technologies like digital ID, verifiable credentials, and blockchain to enhance payments and open banking security and performance
- ensuring robust identity and access management (IAM) to inform and empower customers about their data sharing rights and consent preferences in open banking
- implementing a range of security standards, such as ISO 27001, OWASP Top 10, and PCI DSS, for comprehensive security management

Digital trust and identity in the financial services sector

Digital ID in payments: Digital Identity is an essential part of the solution; however, it also requires careful execution and is best done in partnership with the private sector. India has implemented a biometric digital identity system known as Aadhaar. Its integration with the Unified Payments Interface (UPI) as part of the "India stack" has led to a rapid increase in digital inclusion metrics in India. On the other hand, Aadhaar reportedly suffered multiple breaches that potentially compromised the records of all 1.1 billion registered citizens as of 2019. Other jurisdictions such as Singapore, Thailand, and Hong Kong have implemented sovereign digital ID systems for residents or citizens, while in the Nordic countries, bank-issued digital verifiable credentials such as BankID provide access to government services. Australia is also exploring the development of a digital identity ecosystem that supports interoperability, customer choice, and improved processes across the economy.

Open finance security and trust: Open finance refers to the sharing of client data by data holders with accredited data recipients in the name of increased competition and customer choice. One of the challenges of open finance is to ensure security and digital trust in the consent-based sharing of financial data and payments. To address this challenge, some solutions leverage technologies like digital ID, verifiable credentials, and blockchain to enhance the security and performance of open banking transactions. Others offer a platform for open finance, supporting customer identity verification, consent management, and secure APIs. Such platforms can enable customers to access a dashboard where they can view and manage their data sharing history and preferences.

3.3 Meeting the sanctions screening challenge

To address the sanctions screening challenges outlined in section 2, financial institutions are employing a number of techniques and solutions. However, they rely on conditions that are increasingly in question ranging from data availability to resources. The solutions include:

- advanced AI and machine learning models
- standardized sanctions screening workflows
- advanced data extraction and name matching techniques
- regtech solutions, including utilizing APIs, to accurately model sanctions regimes that differ widely in scope and legal nuance
- integration of blockchain oracles into workflows

Financial institutions are beginning to embrace AI and machine learning driven tools to reduce false positive alerts and prioritize alerts deemed to be higher risk. False positive rates produced by legacy screening systems can reach upward of 95%. EY's experience working with banks across the globe has shown that deploying secondary screening analytics can reduce false positives by up to 70%, allowing investigators to focus on the smaller percentage of payments that truly warrant human review. As importantly, the analytics tools in that study identified additional risks in more than 2% of alerts that an investigator had (incorrectly) marked as false positives.

In addition to those risks, there are questions to be asked as solutions are considered. Can the jurisdiction or entity employ solutions correctly, does it reduce compliance costs, does it reduce barriers to non-banks, does it reduce regulatory complexity, and is there sufficient capital?

Solutions and workflows for sanctions screening

A standardized workflow is a set of steps and rules that define how to perform sanctions screening in a consistent and efficient way. A standardized workflow can help to reduce manual errors, improve data quality, and streamline the screening process.

Name matching technology: blends machine learning with traditional name matching techniques, such as name lists, common keys, and rules, to determine an overall matching score.

Regtech solutions: help to automate sanctions compliance processes and provide audit trails and reports. For example, SWIFT offers a Transaction Screening service that allows financial institutions to screen their transactions against multiple sanctions lists using a single API. Other solutions provide a single screening API that can be configured to match different sanctions regimes and risk profiles.

Blockchain oracles: can enhance the transparency and security of sanctions screening by providing real-time and verifiable data from trusted sources. For example, Chainalysis operates a sanctions screening oracle as a smart contract that validates if a cryptocurrency wallet address has been included in a sanctions designation from organizations including the US, EU, or UN.

4 Opportunities for public and private collaboration

Public-private cooperation and standard-setting around payments fraud, payments ecosystem complexity and open finance, and sanctions screening can foster innovation, security, and interoperability in the financial sector. Standards that foster innovation and responsible risk-taking by providing clear guidance and expectations for all stakeholders involved in the payments value chain can be helpful developments.

Promoting frameworks that balance security, functionality, and interoperability can help foster a harmonized and inclusive payments landscape that supports innovation and competition. Frameworks should also consider the needs and preferences of different customer segments and markets.

The following are examples of initiatives that could help incentivize adoption of advanced measures to address the challenges we have identified.

- **Data gateways:** by growing the size and timeliness of training and production data sets, standardized data sharing gateways across borders and between sectors can improve the power of AI-powered fraud and sanctions screening models, enabling customers to access a wider range of safe and secure payment products and services from different providers, while ensuring data protection and privacy.

- **Data standards:** In areas such as sanctions screening, anti-fraud and open banking, data standardization, including moves to adopt ISO 20022 messaging standards, promise to reduce frictions, payment fails and inquiries, and speed up payments. The FSB recently acknowledged the sanctions screening issue as relevant to cross-border payments in its summary of the first meeting of the new FSB taskforce on legal, regulatory and supervisory issues in cross-border payments (LRS).[1]

- **AI governance frameworks:** developing AI governance frameworks, whether through legislation, standardization efforts, or 'soft law' instruments such as regulatory guidance, will be helpful in clarifying standards and laying down legal and liability regimes in this new, AI-rich environment (see **box**). AI governance can help ensure that AI applications in the payments sector are ethical, transparent, accountable, and fair. AI governance can also help mitigate potential risks and challenges associated with AI use, such as bias, discrimination, and explainability.

Three different 'flavors' of AI governance framework

The European Union's proposed AI Act aims to regulate AI systems through a mandatory and prescriptive approach, focusing on high-risk AI systems in specific sectors such as law enforcement and healthcare. It sets forth six key requirements for high-risk systems, including data quality, technical documentation, and human oversight. This act aligns with existing or proposed EU legislation like GDPR and the Digital Markets Act, aiming to realize human-centric and sustainable development of AI within the EU landscape. The Act is expected to come into force in 2024.

The U.S. National Institute of Standards and Technology AI Risk Management Framework (NIST AI RMF) offers a flexible, voluntary approach to manage AI-related risks across the AI system lifecycle. Unlike the EU AI Act, it is not limited to high-risk AI systems and offers 9 trustworthiness characteristics for AI systems such as accountability, transparency, and safety. The NIST AI RMF aligns with other existing frameworks for information security and privacy, aiming to support the U.S. national strategy for AI and foster international collaboration.

The Monetary Authority of Singapore's (MAS's) FEAT principles are specific to AI in financial services, outlining key principles of Fairness, Ethics, Accountability, and Transparency. While the principles are not legally binding, the MAS expects financial institutions to adopt the FEAT principles as part of their internal governance of AIDA, and to demonstrate how they have applied them in their business activities. FEAT is bolstered by white papers and toolkits published by the MAS-led Veritas Initiative to guide its adoption in financial institutions.

- **Open finance collaborations:** Industry collaboration, and public-private partnerships on emerging technologies, can help leverage the expertise and resources of both sectors to develop and implement innovative solutions for the payments sector in the context of open

[1] The FSB's summary of the first meeting held 10 July states, "Fostering a level playing field among market participants would be a useful route for reducing frictions, by promoting more convergence among and greater clarity and certainty about requirements and supervisory expectations, including as they relate to anti-money laundering and countering the financing of terrorism (AML/CFT), and sanctions screening across the payments chain and jurisdiction."

finance. Such partnerships can also facilitate knowledge sharing, capacity building, and stakeholder engagement, including in open finance. Examples include the Financial Data Exchange (FDX) and Singapore API exchange (APIX) (see **box below**).

Open finance collaborations

Financial Data Exchange (FDX) is a non-profit organization that aims to drive the adoption of open finance in the U.S. and Canada. FDX provides a common standard for the exchange of financial data, called the FDX API, which ensures interoperability, security, and transparency among different parties. FDX also develops user experience guidelines, use cases, certification requirements, and control considerations for data sharing. FDX has over 200 members, including financial institutions, data aggregators, fintech firms, and industry groups.

Singapore API exchange (APIX) is a cross-border, open-architecture API platform that serves as a global marketplace for financial institutions, regulators, supervisors, central banks and fintechs to connect with one another. APIX aims to facilitate innovation and cooperation between financial institutions and fintechs, in effort to digitally transform the banking and financial sectors across the ASEAN region and beyond to ultimately drive financial inclusion.

The Open ID Foundation and Trust over IP, hosted at the Linux Foundation, are two open-source collaborations working on developing digital trust and identity solutions for e-commerce and digital finance.

The UK-based Open Identity Exchange is a technology-agnostic, non-profit trade organization of leaders from competing business sectors focused on building the volume and velocity of trusted transactions online. Through its definition of, and education on, trust frameworks,[2] OIX seeks to create the rules, tools and confidence that will allow every individual a trusted, universally accepted, identity.

- **Privacy regulation:** clarifying privacy regulation to enable data use to train sophisticated models, with client consent, can also improve the efficiency and accuracy of payments processing and fraud detection. Data use should be aligned with the principles of data minimization, purpose limitation, and consent.

- **Model client:** the role of the public sector as a model client can demonstrate the benefits and best practices of adopting new technologies and standards in the payments domain, such as real-time sanctions screening, AI governance, and data harmonization.

- **Data standardization in sanctions screening and anti-fraud systems**: ISO 20022 provides more structured and granular information than previous proprietary standards, which creates an opportunity for the industry to re-think existing approaches to screening and improve data quality and efficiency. Industry stakeholders have put

[2] Trust frameworks include technologies and definitions such as those associated with eIDAS, DIACC, NIST, EDTA, MOSIP, OAuth, FAPI, Trust over IP, etc.

forward several recommendations around sanctions screening processes in the past, including:

- more consistent application of sanctions screening requirements across jurisdictions
- best practices on issues such as complying with list-based sanctions and comprehensive sanctions, importance of a principles-based focus, screening of aliases, whitelisting of false positives, and use of emerging technologies (e.g. machine learning) to reduce false positives
- standardizing sanction list formats, the interpretation of contents, expected responses associated with listings, and list distribution approaches
- increasing uniformity in the list entries and greater use of structured identifiers such as Legal Entity Identifiers (LEIs), Business Identifier Codes (BICs) and digital identities, including in beneficiary information

SWIFT has presented a program for the community to remove sanctions friction through collective action, which includes designing and documenting screening practices and supporting data quality principles for ISO 20022 messages through industry collaboration.

5 Conclusion

Cross-border payments are the lifeblood of the global economy. As the digital transformation of the economy accelerates, the importance of a diverse and secure payments ecosystem, matching different customer needs, increases as well. While policymakers consider key performance indicator targets and central banks explore next generation models for money, it is essential to understand the resources, efforts, and innovation required to keep pace with threats and deliver safe, secure, and trusted payments. Public and private sector institutions both have important strengths to contribute to the effort ensuring that the future of payments matches the needs of a diverse global economy.

Acknowledgement: The IIF would like to thank Visa, Inc. for supporting development of this paper and a related meeting on cross-border payments.

References

ABC News (2023), Experts say AI scams are on the rise as criminals use voice cloning, phishing and technologies like ChatGPT to trick people

ACI Worlwide (2023), Prime Time for Real-Time Global Payments Report

ACFE Insights (2023), AI Fraud: The Hidden Dangers of Machine Learning-Based Scams

BankID, https://www.bankid.com/en/

CNN (2023), AI scam calls: This mom believes fake kidnappers cloned her daughter's voice

Cybersecurity Ventures (2022), 2022 Official Cybercrime Report

European Union, proposed AI Act

EY (2021), Now payments are in real-time, how can Australian banks continue to conduct effective sanctions screening?

Financial Action Task Force (2021), Cross-Border Payments Survey Results

Financial Data Exchange (FDX), https://financialdataexchange.org/

Forbes (2021), Fraudsters Cloned Company Director's Voice In $35 Million Heist, Police Find

KPMG (2023), Pulse of Fintech H1'23

KYC (2021), Solving The False Positives Paradox in Sanctions Screening

IIF (2022), G20 Roadmap to enhance cross-border payments: Industry position paper

IIF and Deloitte (2023), The Ecosystem Imperative: Moving from Open Banking to Open Data

IIF and Deloitte (2023), The Ecosystem Imperative: Embedded Finance

IIF and EY (2023), 12th Annual EY-IIF Bank Risk Management Survey

IIF (2023), Data Policy Impacts – AML and Regtech Solutions

IIF (2023), Data Policy Impacts – Fraud Prevention

IIF (2023), Submission to Financial Stability Board on Third-Party Risk Management and Oversight

IMF (2021), The India Stack is Revolutionizing Access to Finance

McKinsey & Co (2022), Cybersecurity trends: Looking over the horizon

MIT Technology Review Insights (2022), Moving money in a digital world

Monetary Authority of Singapore (MAS), FEAT principles and Veritas Initiative

National Institute of Standards and Technology (NIST), AI Risk Management Framework

Oracle (2019), Disrupting Status Quo in AML Compliance https://www.oracle.com/a/ocom/docs/industries/financial-services/fs-disrupting-status-quo-aml-complaince-wp.pdf

Open IdentityExchange (OIX), https://openidentityexchange.org/

Open ID Foundation, https://openid.net/foundation/

Sanctions.io (2022), The Problem of Name Matching in Sanctions Screening

Sift (2023), Q2 2023 Digital Trust & Safety Index: Fighting fraud in the age of AI

Sift (2023), Growing AI-powered fraud highlights the need for advanced fraud detection

Singapore API exchange https://apixplatform.com/

SWIFT (2023), Small payments. Big opportunity.

SWIFT (2021), Guiding principles for screening ISO 20022 payments

TCS Blog Transforming AML Compliance with RPA

Thomson Reuters (2022), Sanctions screening: Adapting to a growing challenge

Trust over IP, https://trustoverip.org/

Visa (2023), Visa Payment Fraud Disruption Biannual Threats Report December 2022

Visa (2023), MIT_Visa_V6_10052022.pdf (technologyreview.com)

Visa Economic Empowerment Institute (2023), Let's give a voice to end users: Cross-border payments, attributes, and use cases

Visa Economic Empowerment Institute (2023), Meeting the needs of end users: The three layers of cross-border payment solutions

World Economic Forum (2023), Global Risks Report 2023

World Economic Forum (2020), The_Global_Risks_Report_2019

