Future of Financial Intelligence Sharing (FFIS)

Payment Systems Policy Discussion Series

Paper 2:
The case for the G20 cross-border payments reform 'Roadmap' to embed economic crime security by design

January 2024

RUSI

FFIS
Future of Financial Intelligence Sharing

FFIS Policy Discussion Paper

The case for the G20 cross-border payments reform ‘Roadmap’ to embed economic crime security by design

January 2024

About

This Discussion Paper is part of a series intended to support policy-makers and other interested parties to consider the role of payments infrastructure in enhancing the detection of economic crime. This paper has been prepared by the Future of Financial Intelligence Sharing (FFIS) research programme as part of our mission to conduct independent research into the role of public-private and private-to-private financial information-sharing in detecting, preventing and disrupting crime. The FFIS programme is a research partnership within the RUSI Centre for Financial Crime & Security Studies.

Founded in 1831, the Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

Acknowledgements

The FFIS programme would like to thank all those who contributed to this Discussion Paper and our broader research programme. This research project would not be possible without grant funding support from:

- PayTM
- Deloitte LLP
- Verafin
- Synectics Solutions

We are very grateful to all those who have participated in research interviews, research workshops and broader conferences associated to this study.

For more details about the FFIS programme, please visit www.future-fis.com.

Citation and use

This paper is made publicly available and is intended to support a public-interest policy debate related to the effectiveness, efficiency and data proportionality of methods and approaches for detecting and disrupting of economic crime.

All information in this paper was believed to be correct by the author as of 4 January 2024. Nevertheless, the FFIS programme cannot accept responsibility for the consequences of the use of any information contained herein for alternative purposes and other contexts. The views and recommendations expressed in this publication are those of the author and do not reflect the views of RUSI or any other institution.

Author: Nick Maxwell

Reference citation: Maxwell, N., (2024), Payment Systems Policy Discussion Series, 'The case for the G20 cross-border payments reform 'Roadmap' to embed economic crime security by design'. Future of Financial Intelligence Sharing (FFIS) research programme.

Executive Summary:

This second discussion paper in the FFIS *Payment Systems Policy Discussion Series* is intended to facilitate greater dialogue and understanding about risks of a policy disconnection between cross-border payments reform and economic crime security considerations.

This paper forms one of a series of four discussion papers, comprising:

- Part 1: The case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk;
- Part 2: The case for the G20 cross-border payments reform 'Roadmap' to embed economic crime security by design;
- Part 3: The case for the Financial Action Task Force to update and renew the concept of payment transparency; and
- Part 4: The case for international coordination in the use of ISO 20022 for economic crime detection purposes.

In Part 2 of this series, we focus on the case for G20 authorities to embed economic crime security by design in the cross-border payment reform 'Roadmap'.

Since 2021, the G20 has been pursuing a *"Roadmap for Enhancing Cross-border Payments"* which focuses on reducing the cost and enhancing speed, access and transparency of payments across borders. However, overall, there appears to be a lack of joined-up policy thinking between G20-led cross-border payments reform and economic crime security considerations.

The policy drive towards faster and instant cross-border payments threatens to enable fraud and money laundering to be more efficient and to remove a fundamental part of existing processes for ensuring economic crime security: i.e. the opportunity for transaction screening and recall of payments after payment instruction, but prior to cross-border settlement.

Neither the original G20 targets for cross-border payment reform, nor the 2023 consolidated progress report on the Roadmap, nor any aspect of *"Project Nexus"* (the Bank for International Settlements' major technical exercise to enable instant cross-border payments), include any assessment of, or mitigation against, the increased risk of cross-border fraud and associated money laundering inherent in faster cross-border payments.

More broadly, the opportunities to *enhance* economic crime detection effectiveness (in contrast to minimising friction in the speed of payment processes) are not explored to any degree in the payments reform Roadmap.

Our conclusion is that, in the absence of a change of approach, G20-led payments reform process is set to accelerate countries towards the goal of instant cross-border payments without due attention to the fraud and financial crime risks. This is likely to have wide-ranging negative impacts to consumer financial safety, fraud recovery rates, law enforcement effectiveness against money laundering and national security in terms of sanctions implementation.

As a whole and to date, the current G20 Roadmap targets, priority themes and actions appear insufficient to enable integrated and balanced considerations of economic crime risks.

Key recommendations:

While the G20 cross-border payments reform 'Roadmap' targets of cost, speed, access and transparency are important global public-policy goals, we argue that these must be balanced with 'safety'.

We urge the G20 to ensure that payments reform does not create new economic crime vulnerabilities or undermine existing defences against fraud, financial crime and sanctions breach.

We encourage the G20 to ensure that economic crime risks in the existing Roadmap are fully assessed and mitigated against and, indeed, that enhancements to capabilities for the detection of fraud and financial crime available through payments infrastructure are encouraged and developed.

The G20 should endorse a view that the delivery of instant payments should be risk-based, including 'opt-in' safety buffers for additional checks where required.

Our overall recommendation is that, with respect of the G20 Roadmap and on an ongoing basis, 'economic crime security by design' should be integrated at the design stage within the payments reform policy-development process. This recommendation has operational implications for the Roadmap and G20 'priority actions' already in motion. More broadly, this recommendation relates to a change in institutional culture within G20 institutions most involved in payments reform to embrace the concept that economic crime security is a shared responsibility.

The future of payments and the future of economic crime security should go hand in hand. However, at the present time, the inter-governmental policy framework for cross-border payments reform under the G20 is failing to deliver the coordination that is required to assess and respond to economic crime threats inherent in the current Roadmap.

It remains to be seen whether G20 political direction is required to ensure that this failing is addressed and the required policy coordination is achieved.

In the context of fraud, the time may have come for the G20 to spearhead international coordination in response to fraud threats, recognising that such a role complements the existing G20 leadership in payments reform.

For sanctions effectiveness considerations, the G20 will not be a natural home for inter-governmental coordination. Those countries with an interest in financial sanctions effectiveness, such as the G7, will need to re-examine the work-product of the G20 Roadmap and ensure that the implementation of reforms to achieve cross-border payments efficiency does not undermine sanctions effectiveness.

Methodology

This discussion paper series is the product of:

- Open-source research/literature review of relevant materials;
- Policy analysis of research material related to the FFIS 2022 survey process covering 15 private-to-private sharing platforms around the world;
- Critical analysis of discussion at four FFIS project events and three major inter-governmental multi-stakeholder conferences which convened international experts from public and private sectors relevant to the field;[1]
- Additional interviews with key stakeholders;
- Feedback and peer-review on draft versions of the study.

This paper extends on recent landmark publications at the inter-governmental level related to collaborative analytics to tackle economic crime and the role of payments infrastructure in supporting such analysis.

Specifically, this paper builds from:

1) The Financial Action Task Force '*Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing'* best practices paper;[2]
2) The Bank for International Settlements *'Project Aurora'*[3], which established quantitative measures for the value of economic crime analysis taking place at the level of national and cross-border payments infrastructure and the utility/privacy trade-off considerations of use of privacy enhancing technology; and
3) The Europol Financial Intelligence Public Private Partnership (EFIPPP)[4] exploration of the barriers to fraud-risk messaging through payments infrastructure which took place through the Innovation Working Group of EFIPPP from September 2022 to April 2023.

The primary research cut-off period was 4 January 2024 and information should only be taken to be accurate and correct at that time, unless otherwise stated.

Definitions

In general, the scope of threat activity that we consider in this paper is **'economic crime'**[5], which covers activity broader than 'financial crime' or 'white-collar crime' and is used to provide a holistic response to the following types of criminality:

- fraud against the individual, private sector and public sector;
- terrorist financing;
- sanctions contravention;
- market abuse;
- corruption and bribery;
- the laundering of proceeds of all crimes; and
- the recovery of criminal and terrorist assets is also in scope.

In terms of sectoral coverage, the paper is primarily concerned with payment service providers and payment system operators, including central payment market infrastructure systems for settlement and clearing (at the national and international level).

There is no universally agreed definition of terms used in the context of payment systems and central payments infrastructure. In this paper we adopt the following definitions which have been proposed in a comparative analysis paper compiled for the UK's Payment Systems Regulator:[6]

- **Payments system** includes interbank financial market infrastructure whose primary function is to facilitate the exchange of electronic payments for goods and services.
- **Payment system stakeholders** includes the payment scheme rule makers and managers, the technical infrastructure operators and the regulators that together ensure the successful operation of the clearing and settlement of electronic payments.
- **Payment system operator** is a company that operates one or more payment schemes.
- **Central payment infrastructure** is the hardware, software, connections and operations that support the clearing and/or settlement of a payment or funds transfer request after it has been initiated.

This study seeks to draw from experience in two main policy domains of economic crime – anti-money laundering and fraud prevention.

Understanding the case for the G20 cross-border payments reform 'Roadmap' to embed economic crime security by design

The disconnect between the G20 cross-border payment reform 'Roadmap' and economic crime security considerations

What is the "Roadmap for Enhancing Cross-border Payments"?

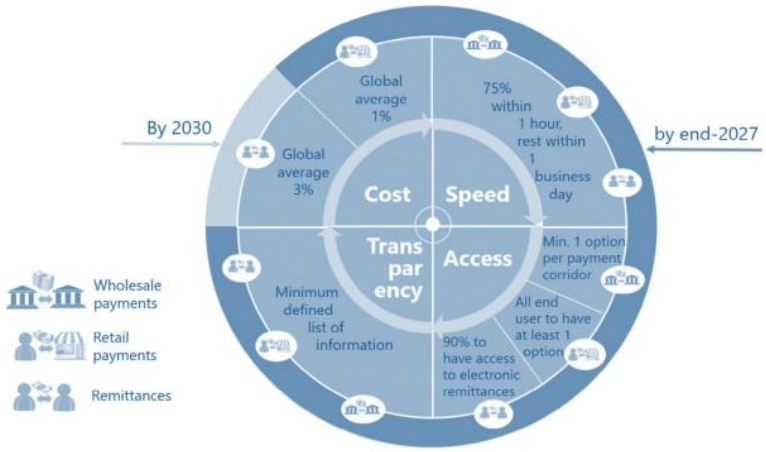
In 2020, the G20 Leaders endorsed a "*Roadmap for Enhancing Cross-border Payments*"[7] based on four targets and 19 "building blocks" for international payments infrastructure reform which is intended to support the global economy in the future.

The main G20 inter-governmental authorities responsible for the delivery of the Roadmap are the Financial Stability Board (FSB) and the Bank for International Settlements (and, largely, the Committee on Payments Market Infrastructures (CPMI) within the Bank for International Settlements), with additional roles for the FATF, the Basel Committee on Banking Supervision (BCBS) and the IMF.

The entire framework is targets-focused, with all subsequent relevant analysis, guidance, working groups, task forces and technical projects commissioned by the G20 authorities being justified in terms of how they support the four targets of the Roadmap.

Specifically, the targets are set out in the graphic below and improvements are largely intended to be achieved by the end of 2027.[8]

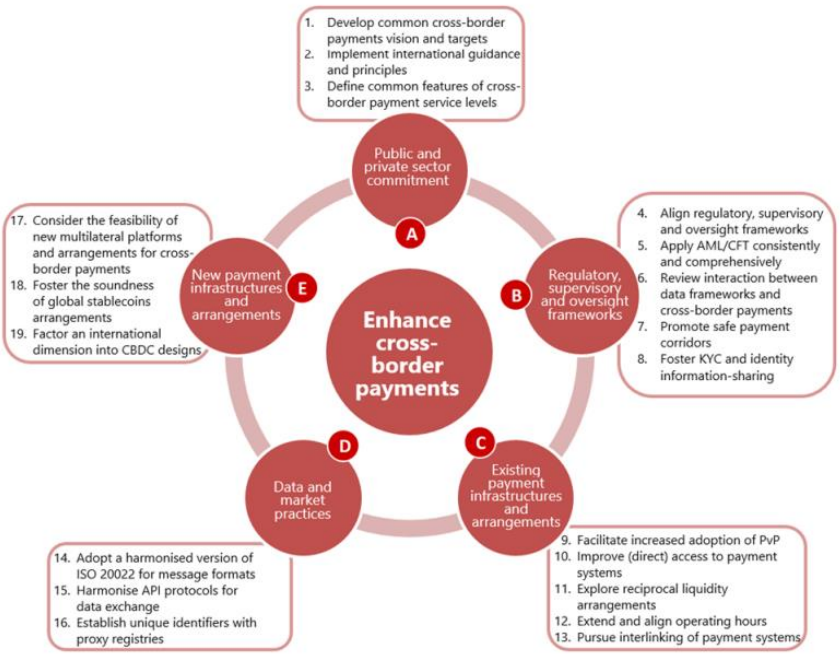
Figure 1. The G20 targets for payments reform



9

The underlying conceptual "building blocks" to deliver the targets are set out across five sections: 'public and private sector commitment'; 'regulatory, supervisory and oversight frameworks', existing payment infrastructures and arrangements', 'data and market practices', and 'new payment infrastructures and arrangements'.

Figure 2. CPMI graphic to describe the building blocks for the G20 Roadmap for Enhancing Cross-border Payments



10

As part of the implementation of the Roadmap, a major initial focus for the G20 authorities has been harmonisation of standards for messaging and API protocols, via the ISO 20022 standard process. This falls under 'Section D' of the G20 Roadmap.

The focus of this FFIS paper engages with 'Section B' of the G20 Roadmap, which includes the following building blocks:

- Building block 4. Aligning regulatory, supervisory and oversight frameworks for cross border payments
- Building block 5. Applying AML/CFT Rules consistently and comprehensively.
- Building block 6. Reviewing the interaction between data frameworks and cross border payments.
- Building block 7. Promoting safe payment corridors
- Building block 8. Fostering 'Know Your Customer' and identity information

It should be noted that, while the targets do not explicitly require instant payments to be delivered cross-border, the practical interpretation of the targets by the Bank for International Settlements and national payment authorities in advanced economies has been to push for payments cross-border to be instant. For example, *'Project Nexus'* is the Bank for International Settlements principal technical project to standardise the way in which domestic payments systems connect to each other. The report title for Project Nexus is "Enabling instant cross-border payments" and the final report concludes that "Nexus could significantly accelerate the growth of instant cross-border payments."[11] The EU legislative proposals to implement the G20 Roadmap, for example, aim to make instant payments in euro available cross-border throughout the EU and EEA.[12]

How does the G20 Roadmap for Enhancing Cross-border Payments recognise economic crime security considerations?

The AML/CFT regime (but not fraud prevention) does feature as a specific building block in the overall Roadmap for Enhancing Cross-border Payments – i.e. "Building block 5. Applying AML/CFT Rules consistently and comprehensively" – and AML/CFT might also be thought to have a strong connection to all of the building blocks in Section B of the Roadmap.

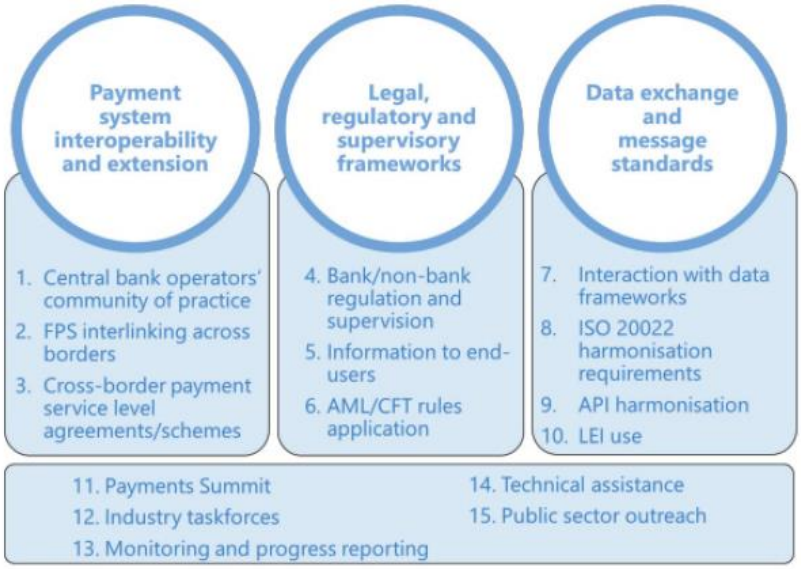
However, despite the titles of the building blocks, published policy thinking to-date associated to the G20 Roadmap by international authorities appears to prioritise efficiency of payments with insufficient attention paid to mitigation of the economic crime security risks associated to faster and instant payments or, indeed, the economic crime detection opportunities associated to new payment systems.

The CPMI and FSB publications relating to aspects of delivering the Roadmap do not engage with the effectiveness of the AML/CFT regime. Instead, FATF is the designated lead for issues relating to the AML/CFT regime. There is no consideration of fraud risks, mitigation or prevention, at any point within the Roadmap or within the subsequent documentation, task forces and guidance related to delivering the Roadmap.

Despite the FATF being a designated lead for Section B building blocks, this mandate within the G20 building blocks is (so far) limited to attempting to achieve greater consistency of AML rules across borders and, thereby, reducing friction and delay in the execution of cross-border payments. Again, the focus is on achieving the original four targets – "enhancing cross-border payments' speed and transparency, while increasing access to cross-border payment services and reducing their costs"[13] – rather than engaging in an in-depth assessment of economic crime security vulnerabilities within the cross-border payments reforms.

More recently, in February 2023, the FSB has released "priority themes and actions" for achieving the G20 targets[14] and reviewed the actions in a consolidated progress report in October 2023.[15] In terms of the priority actions, there are a number of references to the AML/CFT regime (but not to fraud prevention).

Figure 3. The 2023 priority themes and actions for achieving the G20 targets:



"AML/CFT rules application" is a dedicated priority action, and we might expect a strong link to the AML/CFT regime across 'priority actions' 6, 4, 7, 8, 9 and 10 in particular.

However, in terms of the dedicated action relating to the AML/CFT rules – "Action 6: Updating the application of AML/CFT rules" – the October 2023 progress report confirms that the purpose of this Action is to "focus on addressing points where AML/CFT rules, or their implementation, cause friction for cross-border payments, and considering how these could be addressed."[16]

In terms of "Action 7: Enhancing the interaction between data frameworks and cross-border payments", the FSB is required to develop "recommendations, for public consultation, for promoting alignment and interoperability across data frameworks applicable to cross-border payments, including data privacy, operational resilience, AML/CFT compliance, and regulatory and supervisory access requirements".[17] However, once again, it is clarified in the accompanying notes that the principal issue to be resolved is "friction" in cross-border payments: "Action 7 seeks to assess frictions that could arise from these frameworks and consider recommendations that could contribute to achieving the G20's quantitative targets."[18] The FSB is leading this work and the timeline to publish its public consultation report is early-2024 and with a final report scheduled for September 2024.

"Action 10: Exploring enhanced use of the LEI in cross-border payments" contains the only references in the Roadmap documentation to sanctions screening. This is presented in terms of how the adoption of legal entity identifiers could assist with more efficient sanctions screening and customer

due diligence and does not engage with the core principle that instant cross-border payments and straight-through processing threatens to severely negate the effectiveness of sanctions checks.

The broader 'priority theme' on "legal, regulatory and supervisory frameworks" is centred on removing barriers to faster payments, rather than achieving economic crime security. The October 2023 progress report summarises the overall thematic focus as being concerned with how "consistent implementation of Anti-Money Laundering / Combatting the Financing of Terrorism (AML/CFT) controls, including customer due diligence (CDD) requirements, across jurisdictions ***could increase the speed and reduce the cost of cross-border payment services*** [emphasis added]**.** Updating the application of AML/CFT rules under priority action six is an important part of the work under this theme."[19]

Since February 2023, a public-private legal, regulatory and supervisory frameworks taskforce (LRS taskforce) has been created to help engage industry on the actions and issues under this theme.[20]

There is also a planned new (sub-set) action to start in 2024, which forms part of Action 6, which states:

"Promoting the risk-based approach to FATF standards. Following the review of Standards, if necessary, FATF and BCBS, in consultation with CPMI and other stakeholders, to develop guidance to promote consistent and efficient application of the risk-based approach to cross-border payments, including risks relating to new cross-border payment mechanisms."[21]

This part of the Roadmap could be a vehicle for introducing a more balanced consideration of economic crime risks and efficiency objectives, but the details of the workplan were not yet available at the time of preparing this discussion paper.

In summary, the overall objective of all of the G20 authorities work is in supporting the Roadmap targets – i.e. cost, efficiency, access and transparency – which does not currently create clear space to consider economic crime vulnerabilities, nor enhancements to the effectiveness of economic crime detection systems available through payments reform, at the design stage.

Outside of the G20 Roadmap documentation, it should be noted that the BIS has engaged with economic crime issues, including through the following papers:

1) The Bank for International Settlements 'Project Aurora'[22] in 2023, which established quantitative measures for the value of economic crime analysis taking place at the level of national and cross-border payments infrastructure and the utility/privacy trade-off considerations of use of privacy enhancing technology; and
2) The Bank for International Settlements Committee on Payments and Market Infrastructures (CPMI) *"Reducing the risk of wholesale payments fraud related to endpoint security: a toolkit"*, published in October 2019, presents a number of proposals which would be relevant to the G20 Roadmap in terms of fraud prevention. However, as yet, there is no indication that the proposals in the toolkit have been considered or transposed in the context of the Roadmap for cross-border payments.[23]

Where is the gap in payments reform for considering economic crime security?

As described above, the AML/CFT regime does feature in the G20 cross-border payments Roadmap, but the emphasis in the G20 Roadmap, guidance and additional projects and literature is to ensure the AML/CFT regime can be made more efficient and consistent *to facilitate faster* cross-border payments.

The mandate of FATF within the G20 payment reform plan is framed within this context and directed towards the delivery of the four G20 payment reform targets – cost, speed, access and transparency.

The current activities of FATF within the G20 Roadmap do not include examining the vulnerabilities to AML/CFT and sanctions effectiveness arising from the push towards faster, and instant, cross border payments. To date, there is no assessment of these risks within the G20 payment reform Roadmap, Building Blocks, priority themes or priority actions or by any inter-governmental authority connected to the G20.

Fraud is a highly prevalent and pervasive crime type among all G20 countries.[24] Yet assessment, minimisation and mitigation of fraud risk, and associated money laundering, does not feature in the G20 Roadmap at any point.

More broadly, the opportunities to *enhance* economic crime detection effectiveness (in contrast to minimising friction in detection processes) is not explored to any degree in the payments reform Roadmap.

As a whole, the current G20 Roadmap targets, priority themes and actions appear insufficient to enable a mandate for economic crime security analysis.

The potential harm of an unchecked focus on efficiency

As was described in the 2023 FATF Private Sector Consultative Forum, the unintended consequence of making payments faster, cheaper and more inclusive will include a rise in the opportunity for economic crime to take place.[25] Frictionless cross-border, near instantaneous, payments will result in substantial and wide-ranging vulnerabilities for economic crime security.

The current framework for economic crime security in cross-border payments, including in-bound transaction screening and recall of fraudulent payments, relies on the time-gap between payment instruction and settlement.

Law enforcement investigators at the FATF 2023 Private Sector Consultative Forum describe a "golden 72 hours"[26] period that is *potentially* available for investigators to trace and recall stolen funds before they are dispersed after the first cross-border hop in a money laundering chain. This first cross-border transaction, and the gap between payment instruction and settlement, is the principal opportunity in the existing payments architecture to successfully recall fund that have been identified as stolen.

The link between faster payments and faster fraud is well established.

At the domestic level, fraudsters and money launderers are known to make use of faster payments to transfer the relevant funds on to other accounts quickly, reducing the opportunity for an intervention to restrain and recover the funds.

A survey conducted by Aite-Novarica Group, on behalf of Outseer, identified the link between faster payments systems and faster fraud across India, the UK, Malaysia, and Australia.[27] According to the report, "57% of surveyed financial institutions noted an increase in mule activity over real-time payment rails in 2022 compared to 2021. Furthermore, 71% reported an increase in consumer Account Takeover (ATO) using real-time payment rails, while 62% observed a rise in consumer authorised push payment (APP) fraud via real-time payment rails."[28] The authors conclude "These alarming statistics highlight the urgent need for robust measures to mitigate fraud risks within the context of faster payment systems."[29]

The European Payments Council (EPC) *'2023 Payment Threats and Fraud Trends Report'* highlighted that the SEPA Instant Credit Transfer (SCT Inst) feature of "immediate execution followed by immediate clearing and settlement with funds instantly made available to the beneficiary, and continuous processing on a 24/7 basis" was being targeted to support economic crime. [30]

The UK Payment Systems Regulator published in October 2023 its Authorised Push Payment (APP) scams performance report and identified that the UK Faster Payments System was used for 98% of APP fraud payments in the previous year.[31]

The US Faster Payments Council explained "the speed of which the fraud has been carried out is a primary reason why fraudsters are attacking clients on Faster Payments rails."[32]

Box 1. Case study of the impact of instant payments in Brazil on fraud and organised crime.

In Brazil, a real-time payment system called 'Pix' was introduced by the Central Bank of Brazil in November 2020.

Pix has supported a rapid growth in use of digital payments (the stated goal of policy-makers). As the FIS describe in the Global Payments Report:

> *"[In Brazil] Cash represented an* outright *majority (52%) of point of sale transaction value as recently as 2018. The combination of the pandemic and the rise of Pix resulted in that figure dropping to 26% in 2022… Pix transactions are fast (immediate settlement), simple (requiring only the recipient's alias, e.g., a phone number, email address, Taxpayer ID or even an anonymous alias), always available (24/7/365) and cost-effective (free to individuals with nominal fees to businesses). Pix supports a wide variety of use cases such as person-to-person (P2P) money transfers; person-to-business (P2B) payment in physical stores, e-commerce or bill payments; business-to-business (B2B) payment of service providers or suppliers; person-to-government (P2G) or business-to-government (B2G), e.g., tax or utility payments; and government payments to citizens (G2P) such as income tax refunds, social benefits, grants, etc."*[33]

However, as has been widely reported in the media, the rise in Pix instant payments has results in a surge in fraud, organised crime and kidnappings in Brazil.

The Brazilian banking association identified substantial growth in fraud rates since the introduction of Pix, with one in three Brazilians reporting being a victim of financial scams and frauds in 2022, up from one in five a year earlier.[34] Research by Serasa Experian, a Brazilian credit bureau, found that 70% of all social engineering scams were facilitated by Pix in 2021, causing 2.5 billion reais of losses.[35]

Rafael Schiozer, a finance professor at the Fundacao Getulio Vargas, a higher education institution explained in a Reuters article, "Frauds and scams have always existed, but Pix is so fast... and harder to trace. Once it's done, it's done."[36]

The rise in kidnappings has been a particular concern for law enforcement. Brazilian police attributed a 40 percent increase in kidnappings directly to Pix after its first year of roll-out.[37]

The Central Bank of Brazil sought to respond to these issues only after implementation. Measures introduced included daily transfer limits and a cap on transactions conducted during the night to reduce the risk of kidnappings.[38] In addition, the Central Bank has created a shared adverse database for accounts linked to fraud and money mules.[39] These were only introduced after implementation and after the criminality had been observed exploiting the opportunities inherent in the payment system, not at the design stage or with a view to prevention from the outset.

Examples of how the G20 Roadmap is being implemented in legislative proposals place a high degree of reliance on the role of customer screening at the stage of the outbound transaction. However, expert dialogue at FFIS research workshops contributing to this paper and interviews with key stakeholders indicate that this will be insufficient to meet the gap created by the absence of transaction screening and would be entirely inadequate in preventing forms of cyber-enabled fraud or authorised push payment fraud or fulfilling sanctions-related screening obligations.

In the EU roll-out proposals for instant cross-border payments, the legislative proposals related to economic crime security appear to focus on fraud and not the wider realm of financial crime and sanctions. The proposals place a heavy reliance on outbound customer screening through 'Confirmation of Payee' checks to provide economic crime security in place of inbound transaction screening.[40]

Box 2. The EU rollout of instant cross border payments and a conceptual reliance on customer screening.[41]

Delivering on the G20 Roadmap for faster payments, in October 2022, the European Commission adopted a legislative proposal to make instant payments in euro available cross-border throughout the EU and EEA. The emphasis of the legislative proposals is to ensure that payments are "affordable, secure, and processed without hindrance across the EU."

According to the European Commission, "Instant payments seeks to replace traditional credit transfers which are only processed during business hours and arrive at the payee's account only by the following business day, which could take up to three calendar days. Instant payments aims to reduce this time to 10 seconds. The European Commission assess that almost €200 billion euro is locked on any given day in a payment float to wait for clearing and that such monies could be used for consumption or investment in a more efficient manner."

The proposal amends the 2012 Regulation on the Single Euro Payments Regulation (SEPA) and aims to achieve the following:

- Making instant euro payments universally available, with an obligation on EU payment service providers that already offer credit transfers in euro to offer also their instant version within a defined period.
- Making instant euro payments affordable, with an obligation on payment service providers to ensure that the price charged for instant payments in euro does not exceed the price charged for traditional, non-instant credit transfers in euro.
- Removing friction in the processing of instant euro payments while preserving the effectiveness of screening of persons that are subject to EU sanctions, through a procedure whereby payment service providers will verify at least daily their clients against EU sanctions lists, instead of screening all transactions one by one.

In terms of tackling economic crime risk, the current proposals rely on a confirmation of payee requirement:

- "an obligation on providers to verify the match between the bank account number (IBAN) and the name of the beneficiary provided by the payer in order to alert the payer of a possible mistake or fraud before the payment is made."

While 'Confirmation of Payee' obligations are an important element of fraud risk reduction, it is no replacement for removing the safety period for transaction screening and the opportunity for recall of payments identified as fraudulent.

Rather ambitiously, the European Commission state that "payment service providers are expected to make significant operational savings in the area of compliance with sanctions screening obligations as the proposed harmonisation of screening practices of euro instant payments will make this process much more efficient and less dependent on manual work. Operational savings are also expected due to the reduced need to investigate fraud and errors related to instant payments, once the service checking the match between the name and IBAN of the beneficiary is implemented."

In essence, the European Commission is proposing that economic crime security considerations be fulfilled by customer screening and not transaction screening (or any process which may introduce delay in the processing of a payment.)

As such the proposal falls short of being able to mitigate for the increased vulnerabilities to economic crime associated to instant payments.

From a sanctions use-case perspective, the gap between instruction and ultimate settlement is used to investigate cases where insufficient information is available to make an instantaneous decision on a sanction screening obligation.

As part of this FFIS study, regulated entities have reported concern that it will not be realistic to rely on the sender financial institution's screening for sanctions (and permit straight-through processing to their financial institution) without increasing the risk of sanctions breach.

Sanctions requirements, particularly related to U.S. imposed financial sanctions, are much more complex than screening for simple named legal entities and can relate to associated entities, business

sectors and potential use of underlying products – all of which require investigation by inbound receiving financial institutions.

Without the time to screen and investigate inbound payments, financial institutions' ability to screen for sanctions in a comprehensive way will be severely degraded. As such, national security objectives associated to financial sanctions will be compromised.

It is currently unclear how existing compliance and screening functions, which are essential to sanctions, fraud prevention and – to a lesser extent – AML/CFT investigations, will be achieved in a cross-border instant payments framework.

Instances of good practice in individual jurisdictions

As described in Part 1 of this series, there are several instances of national or EU-based payments infrastructure proposals that do incorporate fraud prevention capabilities, without any direction from the G20 payments reform Roadmap.

As a major development in the UK's regulatory approach, Pay.UK are currently developing the UK's New Payments Architecture (NPA) which will support payment providers to access instant payments. Pay.UK is a nonprofit organisation supervised by the Bank of England and regulated by the Payment Systems Regulator and operates most of the payment infrastructures in the UK[42] alongside the Bank of England's wholesale operations, CHAPS, and the real-time gross settlement (RTGS) payment system.

As a coordinated strategy covering 2021-2026, Pay.UK set out to enable more effective fraud detection and better data sharing within the NPA.[43]

Critically, Pay.UK intend to operate the NPA as a vendor neutral platform. As such, Pay.UK will set rules, standards and governance to ensure wider access to payments data to be able to support commercial outcomes.[44] The open nature of NPA also opens up the possibility for multiple vendors offering different analytical services to make use of UK payments data to identify economic crime risks, subject to governance controls.

As a comparable initiative in 2023, though with a more limited capability focused on anomaly detection, EBA CLEARING have developed a pan-European Fraud Pattern and Anomaly Detection (FPAD) functionality and established a developer portal, including a sandbox, to support users in the development and testing of FPAD's application programming interfaces (APIs). In addition to an IBAN/name check, FPAD is intended to provide participants in the network with insights on patterns and anomalies from a central infrastructure level perspective, with anomalies qualified by feedback from participants.[45]

In July 2023, the U.S. Federal Reserve announced that the FedNow Instant Payment Service will include analytical tools to assist participating financial institutions in detecting fraud risk, including[46]:

- The ability for a financial institution to establish risk-based transaction value limits.

- The ability to specify certain conditions under which transactions would be rejected, such as by account number (a “negative list”).
- Message signing, which will validate that the message contents have not been altered or modified.
- Reporting features and functionality, including reports on the number of payment messages that were rejected based on a participating financial institution’s settings.

The Federal Reserve is reportedly exploring “other features that could be made available as part of future releases to aid participants in managing fraud risk, including, for example, value limits that could be tailored to certain uses, aggregate value or volume limits for specific periods (for example, per business day), and/or centralized monitoring performed by the FedNow Service such as functionality that leverages advanced statistical methods and historical patterns to identify potentially fraudulent payments.”[47]

These national level initiatives indicate how capabilities can be established to help prevent against economic crime risks when policy-makers provide such a direction.

From an international perspective, these initiatives are disconnected and developed in an ad hoc manner, jurisdiction by jurisdiction. At the level of cross-border payments, such capabilities – and, indeed, the prioritisation of economic crime capabilities at the design stage – require the support of G20 authorities which are responsible for the cross-border payment reform Roadmap. However, these authorities are tied to the existing G20 cross-border payment reform targets, which – as described above – do not currently allow for, or encourage, activity which is directed towards economic crime security vulnerability assessment or capability maximisation.

A lack of policy coherence to look at fraud and financial crime holistically in the payment reform process

An odd result of the current international governance for payment reform is that there is a significant disconnect between national instances of good practice in economic crime detection (which tend to focus on fraud) and the G20 Roadmap (which makes no reference to fraud). The G20 Roadmap does engage with AML/CFT issues (in terms of aiming to reduce payment friction), but AML/CFT issues are relatively neglected in national payment systems that have developed economic crime detection and prevention measures.[48]

A major part of this challenge is that the FATF has led on international standards for financial crime, but, historically, there has been limited attention on international coordination in how fraud-risk information is shared and acted on.

Table 1. Policy-making architecture and orientation towards fraud or AML regimes

	Fraud detection focused?	**AML focused?**
G20 Building Blocks 'Section' B to link economic crime security to payments reform	No reference to fraud detection or prevention	Yes
National payments level economic crime related analytics where they do exist	Almost entirely focused on fraud detection	Limited to date
International policy-making coordination and standards authorities	Historically, there has been no international policy-making coordination or standards forum	FATF (though covering cyber-enabled fraud in 2022-23)

The policy coordination problems are manifold.

- The G20 leads on payments reform, which has a significant implication for fraud, AML/CFT and sanctions issues.
- No inter-governmental authority currently has a clear mandate to champion fraud mitigation, prevention and detection at the G20 level.
- The FATF leads on AML/CFT standard setting, but the existing mandate within the G20 Roadmap does not extend to examining the vulnerabilities created by the G20 Roadmap.
- While aspects of the sanctions regime rest with FATF, various G7 countries operate independent financial sanctions regimes. For obvious reasons, the G20 does not form a natural home for sanctions effectiveness to be championed alongside the payment reform agenda.
- Meanwhile at the national level, existing instances of good practice in implementing some degree of economic crime detection capabilities within payment systems, described briefly in this paper and in more detail in Part 1 of this series, are largely focused on fraud and not AML/CFT or sanctions capabilities.

The need for a rebalancing the G20 Roadmap to ensure payments reform and economic crime security go hand in hand.

Achieving efficiency improvements to the speed of cross-border payments is undoubtedly an important global policy priority.

The Bank for International Settlements states that "the international network of correspondent banks that facilitates international payments is hindered by high costs, low speed and transparency, and operational complexities."[49] Reducing potential divergence in AML rules between countries to ensure that payments can be as smooth and efficient as possible is also a worthy policy goal and this FFIS paper does not argue for removing the existing G20 targets for speed, transparency, access and cost.

However, overall, there appears to be a lack of joined up policy-thinking between payments reform focused on 'efficiency' and economic crime security considerations focused on 'safety'.

Policy reform to payment systems has a critical impact on economic crime risk threats and vulnerabilities, as well as raising the prospect of enhanced capabilities to tackle economic crime. However, policy-making and public sector technical expertise between payments systems reform and economic crime detection and prevention are fundamentally disconnected at the G20 level.

There is no reference to, or engagement with, fraud risks or fraud prevention objectives in the G20 Roadmap and, where AML/CFT considerations do exist, the emphasis is on reducing friction which might slow down payments.

In the absence of a change of approach, the G20-led payments reform agenda is set to accelerate countries towards the goal of faster and instant cross-border payments without due attention to the fraud and financial crime risks. This is likely to have wide-ranging negative impacts on consumer financial safety, fraud recovery rates, law enforcement effectiveness against organised crime and national security in terms of sanctions implementation.

The G20 Roadmap targets are not incompatible with economic crime security and payment safety, but currently there is no balance between the targets and economic crime security and payment safety considerations at the policy development stage. As a result, all of the subsequent work-flow

of the FSB and BIS / CPMI is driven by the four stated targets of the Roadmap and does not have balancing consideration for economic crime safety built in.

We recommend a risk-based approach to the delivery of cross-border instant payments. We argue that the G20 payments reform authorities need to adopt 'economic crime security by design' as a policy principle in the further development of the Roadmap; integrating that principle into relevant priority 'themes' and 'actions' work in 2024 to 2027. The G20 needs to ensure that fraud risk assessment, minimisation, mitigation, detection and prevention – in particular – is considered at the design stage by G20 authorities rather than left to create widespread harms to society which need to be addressed after implementation.

Those countries (G7 countries in particular) with an interest in the effectiveness of financial sanctions should also ensure that payment reform proposals are compatible with sanctions effectiveness at the design stage before supporting their wider roll-out, rather than relying on the G20 Roadmap in isolation.

Establishing a risk-based approach to the delivery of cross-border instant payments

Not all payments are high-risk enough to require transaction screening and, conversely, not all payments provide a clear benefit to the customer from being settled instantaneously.

Indeed, there may be a strong case for customers who are exposed to, or averse to, fraud-risk to 'opt-in' to a slower-but-safer framework for payments that brings in the opportunity for such screening and recall functionality. Payment stakeholders could potentially develop such functionality as part of an automated risk-based rail selection process at the level of payment service providers.

A US Faster Payments Council White Paper *'Examining Faster Payments Fraud Prevention'* highlights the value in a 24-hour delay for first-time payments as a means of fraud mitigation. [50] The recent U.S. Federal Reserve Bank announcement of the FedNow Service introduced a feature for a financial institution to establish risk-based transaction value limits and other controls in the context of otherwise faster payments.[51]

The deployment of a risk-based approach would allow customers to opt-in to safe corridors for payments and allow for analysis, screening and recall of payments where appropriate from a risk perspective and calibrated to the risks.

Achieving 'economic crime security by design' as a policy principle in payments reform.

Policy making in the future of payments systems must be balanced between payment efficiency and payment safety.

We argue there should be a reorientation in the payments reform, on an ongoing basis, to provide for both efficient *and* safe payment frameworks; ones that can allow a material *increase* in the effectiveness of economic related analysis without excessive reductions in efficiency.

A policy principle of 'economic crime security by design' should be standardised in payments reform, expanding upon the previous focus on speed, cost, access and transparency enhancements and ensuring that AML/CFT issues and fraud prevention considerations are key issues in payments system design.

In practice, we suggest that this should include:

- At the political level, the G20 should require that the further development of the G20 cross-border payments reform plan includes fraud prevention (at the least) as a key design principle, expanding upon the existing G20 payments reform targets.
- The legal, regulatory and supervisory taskforce should lead efforts to ensure that fraud, AML and sanctions effectiveness issues are considered in the context of payment reform, in addition to the general focus on reducing friction in payments. There should be explicit recognition that efficiency is not the sole public-policy interest in cross-border payments and support for the concept of a risk-based roll-out of efficiency improvements, taking into account economic crime safety and security issues.
- The FATF and CPMI should conduct a collaborative evaluation of the potential harm caused by 'instant payment' cross-border initiatives to existing key fraud and financial crime prevention capabilities and develop mitigation processes (including potential for risk-based opt-outs of instant payments for economic crime safety reasons).
- Relevant Roadmap Priority Actions should ensure that they are adequately considering economic crime effectiveness (not just the removal of friction) within the working groups considering data, technical and legal aspects of cross-border payments.
- FATF member countries should ensure that all policy guidance related to payments reform is assessed against economic crime security considerations before being implemented.
- FATF country-level assessors should take active regard to how central bank and payment stakeholders are achieving 'economic crime security by design' in the payments reform process as part of FATF mutual evaluations.

In terms of international forums, there are currently limited forums where considerations about the future of payments and the future of economic crime security come together. To address this and encourage the institutional cultural shift towards 'economic crime security by design' in payments reform, we propose that there should be an annual conference of payment security against economic crime risk, co-organised by the FATF and CPMI and also involving the private sector.

More generally, and on an ongoing basis, national and international payments architecture policy-makers should see their role as being critical to the effectiveness of economic crime detection and disruption systems, as a partner with the private sector and other public sector entities to deliver economic crime security enhancements. This acceptance of shared responsibility for the policy domain of economic crime may require a clear political steer from the G20 for it to take root in the relevant G20 authorities leading current work in the delivery of the Roadmap.

Conclusions

The push towards faster and instant cross-border payments will remove the limited time-period that is currently available for inbound transaction screening and recall of stolen funds before they are settled. This represents a significant dismantling of the current processes to defend against economic crime threats.

As a result, the G20 cross-border payments Roadmap, in its current form, raises substantial fraud and financial crime risks and is likely to reduce the effectiveness of the financial sanctions regime.

There is a fundamental disconnect between those G20 policy-makers responsible for payment system reform and those authorities responsible for fraud prevention and tackling financial crime. This disconnect, enshrined in the current Roadmap targets, is leading to imbalanced policy-making and risks embedding economic crime vulnerabilities within the future of cross-border payment systems.

With a change of approach, the G20 can lead international efforts to protect societies against fraud while also supporting material enhancements to the efficiency of payments processes. These goals are not mutually exclusive, nor necessarily present a trade-off for policy makers. Payment systems can enhance economic crime detection systems.

The principal challenge is one of policy coordination between payments reform policy communities and those with an interest in economic crime security. Beyond policy coordination, there needs to evolve a sense of shared responsibility for economic crime security; one that recognises that the future of payments and the future of economic crime vulnerabilities and capabilities are intimately interlinked.

In this paper we focus on the case that G20 should ensure that payments reform does not create new economic crime vulnerabilities or undermine existing defences against fraud and financial crime, without appropriate mitigation. However, in the broader series of discussion papers, FFIS puts forward a vision that – in addition to mitigating vulnerabilities associated to instant cross-border payments – countries can significantly enhance their capacity to respond to economic crime threats by leveraging the power of payments infrastructure.

In the three other discussion papers in this series, opportunities for policy-makers to be proactive in integrating economic crime security enhancements alongside payment system design are described in more detail, including:

- Part 1: The case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk;
- Part 3: The case for the Financial Action Task Force to update and renew the concept of payment transparency; and
- Part 4: The case for international coordination in the use of ISO 20022 for economic crime detection purposes.

In the context of fraud, the time may have come for the G20 to spearhead international coordination in response to fraud threats, recognising that this complements the existing G20 leadership in payments reform.

For sanctions effectiveness considerations, the G20 will not be a natural home for inter-governmental coordination. Those countries with an interest in financial sanctions effectiveness, such as the G7, will need to re-examine the work-product of the G20 Roadmap and ensure that the implementation of reforms to achieve cross-border payments efficiency does not undermine sanctions effectiveness.

Economic crime vulnerabilities that are created as a result of increased speed of payments should be recognised, minimised, and mitigated against in order to keep societies safe. The G20 cross-border payments reform 'Roadmap' targets of cost, speed, access and transparency are important global public-policy goals, but they must be balanced with 'safety'.

It is our intention that this discussion paper is helpful in spelling out the need for, and the urgency for, economic crime security as a design principle in payment reform.

Abbreviations and Acronyms

AML/CFT	Anti-Money Laundering / Combatting the Financing of Terrorism
APIs	application programming interfaces
APP	Authorised Push Payment fraud
ATO	Account Takeover
BCBS	The Basel Committee on Banking Supervision
BIS	Bank for International Settlements
CDD	Customer due diligence
CPMI	Committee on Payments Market Infrastructures
EEA	European Economic Area
EFIPPP	The Europol Financial Intelligence Public Private Partnership
EPC	European Payments Council
FATF	The Financial Action Task Force
FFIS	Future of Financial Intelligence Sharing
FPAD	Fraud Pattern and Anomaly Detection
FSB	Financial Stability Board
G20	Group of 20 countries
IMF	International Monetary Fund
LRS taskforce	Legal, Regulatory and Supervisory frameworks Taskforce (FSB Secretariat)
NPA	UK New Payments Architecture (Pay.UK initiative)
RTGS	Real-time gross settlement (RTGS) payment system
RUSI	Royal United Services Institute
SCT Inst	SEPA Instant Credit Transfer
SEPA	Single Euro Payments Regulation

Endnotes

[1] Those multi-national events were:
o The 2023 Financial Action Task Force (FATF) Private Sector Consultative Forum (Vienna) 'Payments Transparency' multi-stakeholder discussion session [9 May 2023].
o 'Data Connectivity and 'Whole of System' Thinking in the UK's Architecture to Tackle Economic Crime' FFIS Roundtable (London) [2 May 2023]
o Europol Financial Intelligence Public Private Partnership (EFIPPP) Innovation Working Group (IWG) meeting focused on 'Payments analytics - Building capacity and a community of practice in Europe and beyond' (The Hague) [11 April 2023]
o 'Collaboration to Tackle Economic Crime' Nordic-Baltic Symposium (Stockholm) [3 April 2023]
o The Bank for International Settlements 'Innovation Summit' (Basel) [22 March 2023]
o 'Enhancing Fraud-Risk Alerting Through Cross-Border Payments Systems' FFIS International Practitioner Workshop (London) [15 March 2023]
o 'The Future of Private-to-Private AML Collaboration in Europe' FFIS roundtable hosted in association with Anti-Money Laundering Europe (Brussels) [28 February 2023]
[2] Financial Action Task Force (2022) *"Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing"* - https://www.fatf-gafi.org/en/publications/Digitaltransformation/Partnering-in-the-fight-against-financial-crime.html
[3] Bank for International Settlements (31 May 2023) *"Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders"* - https://www.bis.org/publ/othp66.htm
[4] For overview information of the Europol Financial Intelligence Public Private Partnership (EFIPPP), please see https://efippp.eu/
[5] This paper uses the same definition as laid out in the "UK Economic Crime Plan 2019-2022" i.e. that economic crime refers to a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others.
https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version
[6] Lipis Advisors (2017) *"Fraud prevention and resolution in push payment systems, Comparative analysis"* - https://www.psr.org.uk/media/3dbln5tw/lipis-report-international-fraud-practices-msg_.pdf
[7] CPMI *"Cross-border payments programme"* - https://www.bis.org/cpmi/cross_border.htm
[8] CPMI (July 2020) *"Enhancing cross-border payments: building blocks of a global roadmap: Stage 2 report to the G20 – technical background report"* p10 https://www.bis.org/cpmi/publ/d194.pdf
[9] Lammer T, T Rice (2022) 'The G20 cross-border payments programme: a global effort. Journal of Payments Strategy & Systems Vol. 16, No. 3, 2022, pp. 1-12 reproduced in Financial Stability Board (9 October 2023) "G20 Roadmap for Enhancing Cross-border Payments Consolidated progress report for 2023" - https://www.fsb.org/wp-content/uploads/P091023-2.pdf
[10] CPMI (July 2020) *"Enhancing cross-border payments: building blocks of a global roadmap: Stage 2 report to the G20 – technical background report"* p10 https://www.bis.org/cpmi/publ/d194.pdf
[11] https://docs.bis.org/nexus/introduction/nexus-overview [accessed 4 December 2023]
[12] European Commission (26 October 2022) *"Payments: Commission proposes to accelerate the rollout of instant payments in euro"* - https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6272
[13] CPMI *"Cross-border payments programme"* - https://www.bis.org/cpmi/cross_border.htm
[14] Financial Stability Board (2023) *"G20 Roadmap for Enhancing Cross-border Payments: Priority actions for achieving the G20 targets"* 23 February 2023' - https://www.fsb.org/wp-content/uploads/P230223.pdf
[15] Ibid
[16] Ibid pp 21-22
[17] Ibid pp 22
[18] Ibid pp 22
[19] Ibid pp 12-13
[20] FSB (23 February 2023) Press Release: "FSB invites senior representatives from firms and industry associations to join cross-border payment taskforce" - https://www.fsb.org/2023/02/fsb-invites-senior-representatives-from-firms-and-industry-associations-to-join-cross-border-payment-taskforce/

[21] Financial Stability Board (2023) *"G20 Roadmap for Enhancing Cross-border Payments: Priority actions for achieving the G20 targets"* 23 February 2023' - https://www.fsb.org/wp-content/uploads/P230223.pdf
[22] Bank for International Settlements, *"Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders"* (31 May 2023) https://www.bis.org/publ/othp66.htm
[23] CPMI *"Reducing the risk of wholesale payments fraud related to endpoint security: a toolkit"* (Oct 2019) https://www.bis.org/cpmi/publ/d188.pdf
[24] In the UK "Fraud is the largest crime type with an estimated 3.3 million fraud offences committed in the year ending June 2023" UK Parliament (22 November 2023) Home Affairs Committee - Fraud - Oral evidence - https://committees.parliament.uk/event/19784/formal-meeting-oral-evidence-session/ ; in the U.S. "Fraud makes up 63% of white-collar crimes, making it the most common [crime type]" in https://www.zippia.com/advice/white-collar-crime-statistics/; in Brazil "Almost one in three Brazilians have been victims of financial scams and frauds, a 2022 survey by Brazil's banking association found" in https://www.reuters.com/article/idUSL8N37Z4E1 and "Brazil has 2,800 fraud attempts per minute" in https://valorinternational.globo.com/markets/news/2023/06/25/brazil-has-2800-fraud-attempts-per-minute.ghtml, for example.
[25] Presentation at the 2023 Financial Action Task Force (FATF) Private Sector Consultative Forum (Vienna) "Payments Transparency" multi-stakeholder discussion session [9 May 2023].
[26] Dialogue at the 2023 Financial Action Task Force (FATF) Private Sector Consultative Forum (Vienna) "Asset Recovery" multi-stakeholder discussion session [9 May 2023].
[27] Close, Nathan (2023) Aite Novarica / Outseer *"Faster Payments, Faster Fraud: Examining the Challenges of Faster Payment Systems' Mass Adoption in India, the UK, Malaysia, and Australia"* - https://www.outseer.com/fraud-protection/faster-payments-faster-fraud-examining-the-challenges-of-faster-payment-systems-mass-adoption-in-india-the-uk-malaysia-and-australia/
[28] Aite-Novarica Group / Outseer (2023) *"Faster Payments, Faster Fraud: Solutions To Stop The Madness"*
[29] Close, Nathan (2023) Aite Novarica / Outseer *"Faster Payments, Faster Fraud: Examining the Challenges of Faster Payment Systems' Mass Adoption in India, the UK, Malaysia, and Australia"* - https://www.outseer.com/fraud-protection/faster-payments-faster-fraud-examining-the-challenges-of-faster-payment-systems-mass-adoption-in-india-the-uk-malaysia-and-australia/
[30] European Payments Council (EPC) (November 2023) *"2023 Payment Threats and Fraud Trends Report"* - https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2023-12/EPC181-23%20v1.0%202023%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf
[31] UK Payment Systems Regulator (October 2023) *"APP Scams Performance Report"* https://www.psr.org.uk/news-and-updates/latest-news/news/psr-publishes-first-app-scams-performance-report/
[32] U.S. Faster Payments Council, *"White Paper, Examining Faster Payments Fraud Prevention"* (2020) https://fasterpaymentscouncil.org/blog/4396/Examining-Faster-Payments-Fraud-Prevention
[33] FIS Global, *"THE GLOBAL PAYMENTS REPORT"* (May 2023) - https://www.fisglobal.com/en/-/media/fisglobal/files/campaigns/global-payments-report/FIS_TheGlobalPaymentsReport2023_May_2023.pdf
[34] Feliba, David (June 14, 2023) *"Pix Gangs' cash in on Brazil's mobile payments boom"* Thomson Reuters Foundation / Reuters - https://www.reuters.com/article/brazil-crime-payments-idUKL8N37Z4E1/
[35] Ibid
[36] Ibid
[37] Martins, Cleber [Accessed November 2023] *"A year of pix in Brazil: What does the future of real time fraud look like?"* ACI Worldwide - https://www.aciworldwide.com/blog/a-year-of-pix-in-brazil-what-does-the-future-of-real-time-fraud-look-like
[38] Ibid
[39] Feliba, David (June 14, 2023) *"Pix Gangs' cash in on Brazil's mobile payments boom"* Thomson Reuters Foundation / Reuters - https://www.reuters.com/article/brazil-crime-payments-idUKL8N37Z4E1/
[40] See Box 2. The EU rollout of instant cross border payments and a conceptual reliance on customer screening.
[41] All case study references are from European Commission, *"Payments: Commission proposes to accelerate the rollout of instant payments in euro"* (26 October 2022) - https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6272
[42] Pay.UK consolidated the UK's three national retail payment schemes – the Bankers Automated Clearing System (Bacs), the Faster Payment System (FPS) and the Cheque and Credit Clearing Company (now the Image Clearing System) – into a single retail interbank payment system operator.
[43] Pay.UK *"Our foundation for the future: 2021-26 Strategy"* https://newseventsinsights.wearepay.uk/media/2blffvxk/pay-uk_strategy_document.pdf
[44] PYMNTS *"UK's Payment Strategy Focuses on Fraud Detection, Instant Payments"* (March, 2022) https://www.pymnts.com/news/international/2022/united-kingdom-payment-strategy-focuses-fraud-detection-instant-payments/

[45] EBA Clearing (14 September 2023) *"EBA CLEARING issues specifications and runs analytical pilot for pan-European fraud pattern and anomaly detection"* - https://www.ebaclearing.eu/news-and-events/media/press-releases/14-september-2023-eba-clearing-issues-specifications-and-runs-analytical-pilot-for-pan-european-fraud-pattern-and-anomaly-detection/

[46] U.S. Federal Reserve *"FedNow Service, Fraud and instant payments: The basics"* https://www.frbservices.org/financial-services/fednow/instant-payments-education/fraud-and-instant-payments-the-basics.html

[47] U.S. Federal Reserve *"FedNow Service, Fraud and instant payments: The basics"* https://www.frbservices.org/financial-services/fednow/instant-payments-education/fraud-and-instant-payments-the-basics.html

[48] This is described in more detail in Maxwell, N (2024). Payment Systems Policy Discussion Series, *"Paper 1: The case for national policy-makers to unleash the potential of payments infrastructure to identify economic crime risk"* Future of Financial Intelligence Sharing (FFIS) research programme.

[49] CPMI *"Project mBridge"* https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm

[50] U.S. Faster Payments Council (2020) *"White Paper, Examining Faster Payments Fraud Prevention"* https://fasterpaymentscouncil.org/blog/4396/Examining-Faster-Payments-Fraud-Prevention

[51] U.S. Federal Reserve *"FedNow Service, Fraud and instant payments: The basics"* https://www.frbservices.org/financial-services/fednow/instant-payments-education/fraud-and-instant-payments-the-basics.html