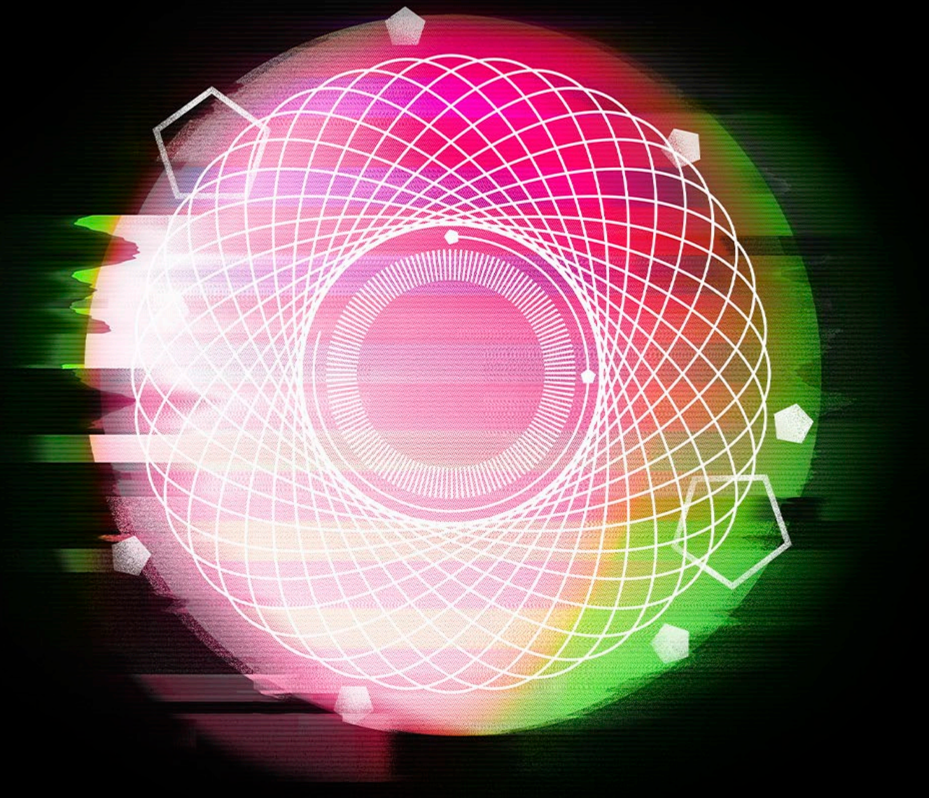
Deloitte.



Leveraging the payments architecture in the fight against economic crime

MAKING AN IMPACT THAT MATTERS since 1845

Table of contents

Executive Summary

Information sharing can help combat economic crime, but is expensive and time-consuming to implement

Money laundering, fraud, and other economic crimes are serious problems affecting our societies. Unfortunately, these issues are exacerbated by the mismatch between the innovative, flexible way in which criminals are able to move money and the typically siloed methods employed by financial institutions, other regulated entities, and the public sector to detect wrongdoing.

There is an increasing focus on constructing information-sharing utilities to address this problem, with some notable examples such as COSMIC in Singapore and TMNL in the Netherlands emerging in recent years. However, before a new utility can brought online, data protection concerns, agreement of common data standards, and the design and implementation of the utility all need to be addressed.[1] This means that substantial time and investment is required before a greenfield utility (i.e. one built on entirely new systems) can start to deliver value.

> Data aggregated within national payments infrastructures may offer a quicker route to generating insights from un-siloed transaction data. In the UK, account-to-account payments data could be used to support law enforcement and regulators across a range of use cases

While this paper agrees that greenfield utilities offer significant long-term potential and should be pursued, it argues that policymakers and practitioners working to fight and prevent economic crime should also look to shorter term routes to the value that information sharing can offer. To do this, they should identify points in the financial system where data is already aggregated, and hence analytics can be run on data from multiple financial institutions without first needing to build an entirely new utility to pool the data. The paper hypothesises that in many countries, the payments architecture could provide such points of data aggregation.

This idea is explored using the UK as an example. The Bankers Automated Clearing System (Bacs) and Faster Payments Service (FPS) are together identified as a possible source of aggregated data for analysis. Both systems enable account-to-account payments, and currently represent around 27% of UK transactions by volume. The transaction data they generate is already used to generate economic crime insights in the form of the Vocalink Mule Insights Tactical Solution (MITS), which alerts subscribing financial solutions of suspected money mule accounts within their portfolios.

[1] Payments Association, 'Data Sharing to prevent Economic Crime: Why you can now share data with confidence', April 2023, pages 8-9

However, there is currently very limited use of the potential of this pooled data to support law enforcement and regulators. In time, use within the private sector could also be extended to support a more effective whole system response to financial crime.

Having introduced the potential of Bacs and FPS data at a high level, the paper sets out three use cases where this data could be used to support law enforcement and regulators at operational, tactical, and strategic levels. Technologically, the paper argues that these use cases are feasible and could be deliverable through alterations to the existing MITS capability, or through coordinating with an alternative provider to provide similar capabilities. Furthermore, if deployed, the use cases could deliver significant benefit. However, the two key obstacles to implementing the use cases are commercial and legal. For the former, the paper identifies possible sources of funding that could be used to bear any costs falling on the public sector. For the latter, the paper urges stakeholders from law enforcement, Pay.UK (the UK's leading retail payments authority), financial institutions and other key stakeholders to come together and discuss the possible routes forward to address any legal risks posed by the use cases.

The UK's New Payments Architecture programme further increases the potential of using payments system data to combat economic crime. However, a public sector-led strategy is required to ensure this opportunity sits within a coherent network of information-sharing utilities for the future

The benefits that can be realised in the short-term from use cases based on Bacs and FPS data should be further increased when the UK's New Payments Architecture (NPA) programme terminates (full implementation currently scheduled for June 2026) and has delivered a refresh in the UK's retail payments infrastructure. The NPA, through its incorporation of the ISO 20022 data standard – and the ability it will provide third parties to develop value-add payments services using its underlying data - will provide a richer and more accessible pool of data for use in analytics. However, the paper notes that it is important for anti-economic crime policymakers and practitioners to play an active role as the NPA is further designed and developed, to leverage the full potential of this 'once in a generation' opportunity.

Finally, the paper notes the importance for countries of cohering the various information-sharing initiatives taking place within their borders under an overarching strategy, and therefore welcomes the announcement in the UK's second Economic Crime Plan 2023-26 that the government seeks to create a public-private economic crime data strategy. The paper touches on some key considerations this strategy should seek to cover. For example, it is crucial to maximise the data coverage offered by utilities, and that competing utilities are not allowed to inadvertently become data siloes themselves. Moreover, the strategy should consider how non-traditional financial data, such as that generated by crypto exchanges or social media sites, can be more effectively shared, as well as seeking to lay the groundwork for better international information sharing. The strategy should also set out how it will bring in the private sector to move this agenda forward, finding ways to leverage its capacity to compete and innovate whilst ensuring these forces remain focused on key strategic targets. The use of structured, technological competition and the wider replication of the NPA's overlay services model - which seeks to create an ecosystem that is simultaneously secure, rich in the data it provides, and able to sustain a wide array of analytics service providers - are both routes to consider.

1: Introduction

The primary focus of this paper is to assess how data aggregated within the UK payments architecture could be used as a form of information-sharing utility to combat money laundering.

For the purposes of this paper, we define information-sharing utilities as mechanisms that either allow duplicative processes to be undertaken once on behalf of many (e.g. Know Your Customer (KYC) utilities), or which allow otherwise siloed datasets to be brought together (both public-to-private and private-to-private), either through data pooling, or through the use of collaborative analytics, to enhance the efficiency and effectiveness of risk management functions. The terms information-sharing utility, platform, and mechanism will be used interchangeably to refer to this concept throughout the paper.

Among anti-money laundering (AML) and other anti-economic crime practitioners, there is increasing interest in information-sharing utilities. The pooling and analysis of data from across multiple Financial Institutions (FIs) and other Regulated Entities generates better insights into criminal money laundering networks and other types of economic crime than can be achieved through siloed data analysis. However, it is complicated and time-consuming to agree the standards, protocols, and legal basis through which information sharing can take place.

As such, *existing* points of data aggregation in the financial system where data from across multiple FIs already resides in one place may provide the opportunity to realise the benefits of information-sharing utilities more quickly and should be considered as an alternative or complement to building greenfield data-pooling platforms.

The UK payments architecture is one of these points of data aggregation. Furthermore, Action 25 of the UK's first Economic Crime Plan 2019-22 (ECP1) has previously called for greater consideration around the use of payments systems to tackle economic crime;[2] the recommendations within this paper are in line with that intent.

While AML is the primary focus of the paper, it will be noted where recommendations could also have an impact on fraud, which has increased significantly in England and Wales, now accounting for 41% of all recorded crime.[3] The use cases chosen for exploration in this paper could equally have been dedicated primarily to anti-fraud measures; indeed, in June 2023 Pay.UK announced a pilot in which three private partners will use FPS transaction data to identify suspicious activity and compare it to known fraudulent behaviours.[4] However, the last few years have been notable for the emergence of several high-profile AML-specific information-sharing pilots, which had previously been scarce. This paper therefore chooses to link into this latest field of innovation, hence choosing as its focus the use of payments architecture data against money laundering specifically.

Although the paper discusses the UK's payments architecture and provides UK use cases, the arguments made here could apply equally in other jurisdictions. Indeed, any jurisdiction where data is aggregated within national payment systems may have lessons it could draw from the proposals laid out here.

[2] https://www.gov.uk/government/publications/economic-crime-plan-2019-to-2022/economic-crime-plan-2019-to-2022-accessible-version

[3] House of Commons Committee of Public Accounts, 'Progress combatting fraud', March 2023, page 3

[4] https://newseventsinsights.wearepay.uk/media-centre/press-releases/payuk-partners-with-visa-synectics-solutions-and-featurespace-on-pioneering-fraud-detection-and-prevention-initiative/

The problem of money laundering

Global money laundering is a significant problem facing the financial system. While its true value is hard to calculate, estimates put forward are consistently large: globally, the UN Office for Drugs and Crime has estimated the amount of money laundered annually at 2% - 5% of global GDP, which would put it at between $1.9 and $4.9 trillion in 2021;[5] [6] within the UK, the government's most recent National Strategic Assessment for Serious and Organised Crime acknowledged that "[it is] a realistic possibility that the scale of money laundering impacting the UK (including through UK corporate structures or financial institutions) is in the hundreds of billions of pounds annually."[7]

The financial flows alone do not tell the whole story; organised crime groups and kleptocrats, whose crimes generate much of the money that is eventually laundered, pose an increasingly clear threat to the sustainable development of our societies.

At a human level, a UN report has estimated that 50 million people were in a situation of modern slavery each day in 2021, amounting to 1 in every 150 people worldwide. Money laundering will continue to enable criminals to benefit financially from this crime, which has been growing in prevalence since the UN's last estimate in 2017.[8]

At a national level, the UK Parliament's Foreign Affairs Committee has noted the impact economic crime has had both on the UK's institutions and Ukraine's territorial integrity, stating in 2022 that the "consequences [of illicit finance] for [UK] national security and the integrity of [UK] institutions and services are laid bare by the current war in Ukraine; assets laundered through the UK are financing President Putin's war in Ukraine."[9]

And at a global level, despite the existential threat posed by climate change, criminals are taking advantage of the "low risk, high reward"[10] appeal of illegal logging, wildlife trafficking and other offences to commit serious environmental crime and launder the proceeds.

Given the widespread nature of these crimes and the damage they inflict, it is clear that tackling money laundering effectively is critical - in helping to prevent criminality and deter criminals; in providing opportunities to disrupt and break up criminal networks; and, in recovering criminal assets and returning it to victims.

Despite the recognition of these issues and a clear desire in the private and public sectors to combat them, success has been limited. Recent estimates suggest that $274.1 billion was spent on financial crime compliance in 2022,[11] and yet a recent roundtable of experts concluded that less than 1% of criminal proceeds are ever confiscated.[12]

Ultimately, the current AML system is not fit for purpose. Criminals are able to launder money through complex, multi-institutional and multi-jurisdictional schemes. Detecting these schemes requires collaboration and coordination between private and public sector stakeholders. Removing silos between data sets is fundamental. But currently, sharing information between organisations is challenging.

Among FIs, banking confidentiality and data protection legislation rightly mean that clear safeguards must be applied to personal data and that any instances of information sharing must have a clear purpose and proportionality.

[5] https://www.unodc.org/unodc/en/money-laundering/overview.html
[6] https://data.worldbank.org/indicator/NY.GDP.MKTP.CD
[7] National Crime Agency, 'National Strategic Assessment of Serious and Organised Crime 2021', May 2021, page 55
[8] International Labour Organisation, Walk Free, and International Organisation for Migration, 'Global Estimates of Modern Slavery: Forced Labour and Forced Marriage', September 2022, pages 1-5
[9] House of Commons Foreign Affairs Committee, 'The cost of complacency: illicit finance and the war in Ukraine', June 2022, page 3
[10] Financial Action Taskforce, 'FATF Report: Money Laundering from Environmental Crime', June 2021, page 3
[11] https://risk.lexisnexis.com/global/en/insights-resources/research/true-cost-of-financial-crime-compliance-study-global-report
[12] https://www.fatf-gafi.org/en/publications/Fatfgeneral/Outcomes-fatf-plenary-october-2022.html

However, this has left FIs uncertain about when they *can* share data, given the legal risks of getting that judgement wrong. As such, while FIs and other regulated entities with AML regimes monitor transactions originating in their own accounts, it is difficult for them to access the wider information from one another which could reveal when an apparently innocuous payment should be considered highly suspicious.

As for LE, while the emergence of public-private partnerships such as the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) has helped LE to improve its dialogue and information and intelligence exchange with private sector parties, there is still more that can be done. For example, wider information-sharing research has noted the opportunity for more systematic public sector feedback to increase FI transaction monitoring effectiveness. Currently, FIs report suspected money laundering cases to LE but are not consistently informed whether these cases are later confirmed as money laundering or not. Without this input, FIs find it more difficult to refine their understanding of criminal typologies. This in turn restricts their ability to adjust monitoring procedures and thereby generate more true and fewer false positives.[13]

Equally, LE could more directly signpost the formats in which it would like to receive FI data. This would increase its efficiency in acting on the information it receives, spending less time arranging data and more time analysing it, thereby generating insights more quickly.

LE *is* seeking to further enhance its engagement with FIs and the private sector, but the capacity that can be deployed in this area is limited. Indeed, the UK Parliament's Foreign Affairs Committee issued a call in 2022 for "a substantial increase in funding and expert resourcing for the National Crime Agency, Serious Fraud Office and other responsible agencies."[14]

For now, LE capacity, the legal risks and uncertainties faced by FIs (noted above), and other factors (e.g. a lack of regulatory incentivisation), mean that the potential of public-private information sharing has not been fully realised and might still be considered a strategic weakness in the UK's AML response.

The result is that the UK has an overarching AML ecosystem where between them, a diverse set of stakeholders *do have* much of the information they need to disrupt criminals and recover assets but arranged in a way that inhibits the speed of sharing and insight required for successful intervention.

This lack of connectivity creates a fundamental mismatch in operating capability between the money launderers and those trying to stop them, regardless of the significant sums FIs are spending on their internal AML controls.

The promise of information sharing

Fortunately, a shift in this inherent mismatch between criminal practices and AML techniques is emerging. Information sharing by FIs, both with one another and with LE and wider government, has garnered much attention over the previous decade across policy, pilots, and full implementation.

At a policy level, FATF consolidated its existing information-sharing standards in 2016 to provide clarity on its requirements in this area[15] and has continued to release reports on how this field is developing, drawing on the latest examples from around the world.[16] Numerous pilots have taken place globally, such as the TriBank pilot in the UK which saw three major UK banks pool encrypted data into a centralised transaction monitoring utility. And in some jurisdictions, fully-developed information-sharing utilities are now being constructed: Transactie Monitoring Nederland (TMNL) has scaled an approach similar to that in the UK TriBank pilot, combining anonymised transaction data from across several FIs and applying

[13] Maxwell, N., A Survey and Policy Discussion Paper: 'Lessons in private-private
financial information sharing to detect and disrupt crime', Future of Financial Intelligence Sharing (FFIS)
research programme, July 2022, page 32

[14] House of Commons Foreign Affairs Committee, 'The cost of complacency: illicit finance and the war in Ukraine', page 11

[15] Financial Action Taskforce, 'Consolidated FATF Standards on Information Sharing', June 2016

[16] Financial Action Taskforce, 'Stocktake on Data Pooling, Collaborative Analytics and Data Protection', July 2021; Financial Action Taskforce, 'Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing', July 2022

specialised algorithms to detect suspicious activity;[17] and the Monetary Authority of Singapore (MAS) is developing COSMIC, a platform which will enable six major FIs to share information on customers exhibiting multiple red flags[18].

Despite this growing momentum, information-sharing utilities are by no means straightforward solutions to execute. Turning to the UK, in February and March 2023 a payments industry body white paper surveyed its members to understand the barriers preventing FIs from sharing data. The top three reasons, all of which were selected by more than 50% of respondents, were (1) data protection concerns, (2) lack of industry data sharing mechanisms, and (3) lack of industry-wide data consistency.[19]

Positively, as the paper explains, data protection concerns (and relatedly, banking confidentiality issues) are set to be eased respectively by the Data Protection and Digital Information Bill (DPDI) and the Economic Crime and Corporate Transparency Bill (ECCT), both of which are passing through the UK Parliament at the time of writing.[20]

As for establishing a data-sharing mechanism and embedding industry-wide data consistency, TMNL and COSMIC illustrate that, in certain countries, FIs and the public sector are attending to these gaps. The UK is among these: the Home Office and UK Finance are facilitating a pilot to enable FIs to share data on customers that pose the highest economic crime risk, and the Cabinet Office is developing a "Single Network Analytics Platform (SNAP) for cross-government and UK banking sector use."[21]

However, even though the three biggest obstacles identified by the survey are being addressed, significant challenges remain before AML value will be realised. As delivery programmes progress, there will be difficulties in reaching agreement across participating FIs (many of whom will have different risk appetites) in terms of who will operate the mechanism, what data fields will be required, what the cybersecurity and data protection processes should be, and what use cases will be developed once the data is pooled. Similarly, the operational data across a group of FIs will inevitably exist in several different standards, so there will be complications in creating a harmonised dataset. The work required to solve these problems, which can be typical with greenfield initiatives, delays the point at which data will be aggregated and consequently the point at which FIs and LE will benefit.

Therefore, while steps to build bespoke information-sharing utilities such as SNAP are encouraging and it is important that due care and time is taken for their implementation, AML stakeholders should also look for places where data is already aggregated as a faster means to realise information-sharing benefits by avoiding or reducing the upfront challenge of first needing to bring data together.

In the UK, the Payments Architecture offers one such point of data aggregation, and within it, the data held by Pay.UK in particular. This paper sets out the case for leveraging its potential focusing on public-to-private use cases, that is, using privately held transaction data to support LE and regulators in disrupting criminal networks and recovering assets. As we set out, Pay.UK's data is already being used in private-to-private use cases, so it would a logical next step to extend its benefits to the public sector.

Before moving on to look at the UK payments architecture in the next section, it is important to reiterate that the primary rationale behind this paper's proposals is speed: it will be quicker to derive insight by analysing data that is already pooled than it will be to pool data and then analyse it. The paper does not suggest that this approach would lead to more effective solutions than would be offered by greenfield platforms in time; it contends only that it would deliver at least *some* benefit more quickly.

[17] https://tmnl.nl/en/

[18] https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic

[19] Payments Association, 'Data Sharing to prevent Economic Crime: Why you can now share data with confidence', April 2023, pages 9

[20] *Ibid*., pages 13-15

[21] https://www.contractsfinder.service.gov.uk/notice/784bacfd-8840-4b19-b3ed-1bdcc021a621

This may appear a limited ambition, but in the current landscape, any benefit from information sharing could prove transformational – not just in pure LE outcomes such as arrests, assets recovered etc., but in bringing momentum to the wider information-sharing movement and providing lessons for the greenfield utilities of the future.

Before moving on to look at the UK payments architecture in the next section, it is important to reiterate that the primary rationale behind this paper's proposals is speed: it will be quicker to derive insight by analysing data that is already pooled than it will be to pool data and then analyse it. The paper does not suggest that this approach would lead to more effective solutions than would be offered by greenfield platforms in time; it contends only that it would deliver at least *some* benefit more quickly.

This may appear a limited ambition, but in the current landscape, any benefit from information sharing could prove transformational – not just in pure LE outcomes such as arrests, assets recovered etc., but in bringing momentum to the wider information-sharing movement and providing lessons for the greenfield utilities of the future.

2: The UK Payments Architecture

Overview

Naturally, when individuals are spending money, their focus is on what the money is for, who the recipient is and how much they are spending; people rarely stop to dwell on how the payment itself is made. But by looking into that 'how', a UK resident would realise that in a typical month they use several different payment 'rails'. For example, when buying food from the supermarket, they might typically pay by card, whether with the physical card or through software such as Apple Pay and Google Pay. They receive their salary via Bacs Direct Credit and settle regular bills through Bacs Direct Debit. In ad hoc payments between friends and family, they might make transfers using FPS. They might also occasionally withdraw cash from an ATM. Without much concerted effort, they have used four different payments rails.

Figure 1 – An overview of the UK Payments Architecture (2021) [22] [23]

Payment Type	Operator	Volume (annual transactions in millions)	% of total
Card	Various (e.g. VISA, Mastercard, AMEX)	**22,900**	**57**
Bacs	Pay.UK	**6,500**	**16**
Cash	LINK	**5,900**	**15**
Faster Payments	Pay.UK	**4,200**	**10**
Cheque	Pay.UK	**150**	**0.4**
CHAPS	Bank of England	**50**	**0.1**

[22] UK Finance, 'UK Payment Markets Summary 2022', August 2022

[23] Deloitte Analysis

Figure 1 provides an overview of the UK's payments architecture. It is not exhaustive – for example, it does not cover emerging "By Now, Pay Later" payments rails (which in practice can go over existing rails), but nonetheless covers >98% of UK transactions in 2021 by volume. Clearly, even in this simplified depiction, the UK Payments Architecture is a complicated system, and its data is fragmented across several different pieces of infrastructure.

While this paper is making the case for leveraging data that is already pooled, considering how the data from the different rails above could be brought together is not in scope; we instead focus on the existing pool of data within these rails that has the most promise for AML use cases. As will be shown below, such promise is clearest in the Bacs and FPS systems, which, while separate rails, provide a source of aggregated data, driven by the fact that both rails are operated by the same provider on behalf of Pay.UK and that that provider is already able to pool Bacs and FPS data together[24] (though it is recognised that the data remains 'owned' by the relevant bank). As shown in Figure 1, Pay.UK also operates the Image Clearing System (ICS) which processes cheque transaction data. However, this will be omitted from further discussion, due to its low volume and the fact that the capability does not currently exist (although it could be created) to analyse ICS data alongside Bacs and FPS.

The potential of Pay.UK's data

There are several features of Pay.UK's Bacs and FPS data that make it a potentially transformative source of insight for LE regarding money laundering in the short term. The data contains useful data fields which can be accessed from one source and is already being processed for anti-economic crime use cases. It also represents a significant proportion of UK payments volumes.

Bacs and FPS transaction data comprises actionable data fields for AML use cases that do not need enrichment from external data sources. As a minimum, these two systems record the time and value of transactions, as well as sufficient data to directly identify the sending and receiving accounts if required. This contrasts with card payments, for example, where often the card network will record the time, value, and location of the transaction alongside a range of other fields, but the FI issuing the card would then be required to input if the payment needed to be linked back to a bank account.

Bacs and FPS data is also already being used to support an anti-economic crime capability. Vocalink developed the Mule Insights Tactical Solution (MITS) proposition in partnership with Pay.UK in 2018: "MITS technology…traces illicit funds as they move between bank and building society accounts regardless of whether the payment amount is split between multiple accounts, or those accounts belong to the same or different financial institutions." In essence, FIs signed up to MITS are alerted when suspected mule accounts are discovered within their portfolios and receive dispersion tree visualisations illustrating the nature of the unusual activity.[25] That this use case, based on FPS and Bacs data, already exists increases confidence that others will also be possible.

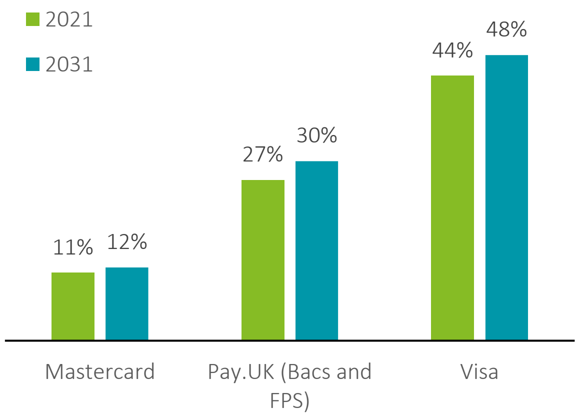
Finally, Bacs and FPS data has volume, representing a significant proportion of UK transactions. As seen in Figure 2, the Bacs and FPS rails currently carry around 27% of UK transactions by volume, set to grow to 30% by 2031. This puts them second in the UK by volume of payments behind VISA with its debit and credit cards network (44% of UK transactions in 2021, forecast to reach 48% in 2031).

In addition, while the UK Finance forecasts which are the basis for these numbers provide an authoritative base case, there is uncertainty around how the payments market could change over the next ten years. One emerging payments method is "Request to Pay". This has already been launched, and – whether in a B2B, B2C, or other context – enables billers to request a specific payment amount from payers, who then make an account-to-account payment in response.[26]

[24] https://www.wearepay.uk/what-we-do/
[25] https://www.vocalink.com/newsroom/success-stories/case-study-mits/
[26] https://www.requesttopay.co.uk/

While rates of adoption are hard to predict, it is possible that some card payment volume will move to the Request to Pay framework or to other innovative account-to-account payment solutions that emerge in future. “As such, Faster Payments could become an alternative to card payments”[27] notes UK Finance. If this change occurs, the Bacs and FPS combined share of UK transactions could well surpass the 30% currently forecast for 2031, suggesting that possible insight offered by these payment rails will only increase in value over time.

Figure 2 – Share of UK payments volumes, 2021 and 2031[28] [29] [30]



In summary, Bacs and FPS provide a high volume of data that can be put to use in anti-economic crime use cases. For all these advantages, a different dataset which covered a higher proportion of the UK’s transactions, across more payment rails, and with clear access to KYC information, would generate more insights and have the potential for more use cases. For example, the identification of money laundering techniques where criminals acquire a merchant’s details for the processing of card payments would be more easily detected in a platform with access to card provider data, as would laundering through pre-paid cards.

However, as discussed previously, this paper is focused on the quickest routes to usable, pooled data, and as noted, bringing together diverse pools of data at any scale necessarily takes significant time and investment. Through MITS, Bacs and FPS data is already generating anti-economic crime insights for participating FIs. There are clear, current opportunities to extend that potential to the public sector, as will be demonstrated through the use cases in the following section.

[27] UK Finance, ‘UK Payment Markets Summary 2022’, August 2022, page 6
[28] UK Finance, ‘UK Payment Markets Summary 2022’, August 2022
[29] https://www.statista.com/statistics/817351/leading-brands-in-payment-cards-in-the-united-kingdom/
[30] Deloitte Analysis

3: AML use cases

This section sets out three possible use cases where the public sector could draw on FPS and Bacs data for insight. This is a non-exhaustive list, but the use cases presented illustrate the potential for this data to address operational, tactical, and strategic issues in the public sector's fight against crime.

1. **Tactical enquiry following a SAR or other lead** – Law Enforcement / Financial Intelligence Unit requests FPS and Bacs data to understand the network of payments surrounding an account identified by a recent SAR, or to piece together the known associates of a suspect in a non-SAR-related case
2. **Strategic assessment of impact of LE / regulatory interventions** – Law Enforcement / regulators have intervened to address a money laundering loophole in the financial system. They request FPS and Bacs data to estimate the impact this intervention has had
3. **Operational capability to monitor for a specific ML typology** – Law Enforcement has identified a high priority ML typology to combat which will likely escape detection by individual FI transaction monitoring. Algorithms are developed to monitor for this centrally in FPS and Bacs data, with LE alerted upon detection

For each use case, a current AML issue will be discussed, followed by how the use case overcomes the issue, the benefits it delivers, and how technologically feasible it will be to implement. This is followed by a survey of the commercial and legal obstacles which are common across the three use cases, and which need to be addressed before any use case can be mobilised.

Finally, before viewing the use cases, it is important to note that all three rely on an analytical capability that can manipulate and analyse FPS and Bacs transaction data. Currently, as has been noted above, Vocalink provides a partially analogous role through its MITS proposition. However, if the relevant permissions were given, it is possible that other providers could expand this function and develop new ones through access to the central data pool. Indeed, in June 2023 Pay.UK publicly announced a pilot in which a number of different organisations are developing a fraud detection service based on FPS data.[31] Likewise, the planned construction of the New Payments Architecture (discussed in section 4) should, if shaped correctly, further open up opportunities for more vendors to use payments data in economic crime analytics solutions. This is likely to be positive, as competition gives more options for taking the use cases forward, could stimulate further use cases, and is likely to drive higher performance at better prices. Therefore, if the use cases presented in this paper were pursued, a range of providers could be used to enable them. We do not address this topic per se in this paper, and therefore the explanation of each use case will refer neutrally to "the data analytics provider", in order not to pre-judge which organisation(s) this might be.

Conversely, when assessing the feasibility of the use cases, each of their technological requirements will be compared against existing FPS and Bacs analytical capabilities, as these give the best indication of what is and is not currently possible.

[31] https://newseventsinsights.wearepay.uk/media-centre/press-releases/payuk-partners-with-visa-synectics-solutions-and-featurespace-on-pioneering-fraud-detection-and-prevention-initiative/

Use Case 1: Tactical enquiry following a SAR or other lead

Current AML Issue

The Suspicious Activity Report (SAR) regime is a critical plank of the UK's AML efforts. A SAR is "a piece of information alerting law enforcement agencies that certain client / customer activity is in some way suspicious and might indicate money laundering or terrorist financing". Persons in the regulated sector, such as staff within FIs, are required under Part 7 of the Proceeds of Crime Act (2002) and Terrorism Act (2000) to submit a SAR should they "know, or suspect, or have reasonable grounds for knowing or suspecting" these suspicious activities.[32] SARs, once submitted, are routed to the UK's Financial Intelligence Unit (FIU) within the NCA, at which point a SAR may be taken on for further investigation by LE or by the FIU itself.

As noted in the introduction, currently FIs (both globally and in the UK) are highly constrained in what data they can share with one another, and while a new information-sharing gateway was opened up in the UK through the Criminal Finances Act 2017, its use has been "extremely limited since its establishment" as the threshold for sharing was set too high "at the standard of 'suspicion', whereby a regulated entity will have already met the threshold to file an individual suspicious activity report."[33] Therefore, although it is commonly accepted that FIs would be better able to identify criminal activity by combining their data and monitoring for *networks* of suspicious accounts, this practice is currently limited – FIs produce SARs based only on activity they can see in their own portfolios of accounts, which results in two clear issues.

First, it leads to a high number of SARs, which are of varying quality, and which overburden LE. Given their partial view of payment flows, FIs are not optimally positioned to identify suspicious activity. They are also wary of punishment by regulators for shortcomings in AML controls, as has happened recently with Santander (fined £107.8m in 2022),[34] HSBC (fined £63.9m in 2021),[35] and NatWest (fined £264.8m in 2021).[36] Taking these two things together – i.e. a structurally disadvantageous position from which to identify money laundering, coupled with significant penalties for failing to do so – FIs are effectively incentivised to set a low threshold of what they consider 'suspicious' and to therefore defensively report a high number of SARs.

Given the limited resources within LE to respond to SARs, this inevitably leads to difficult prioritisation decisions regarding where to place investigative resources to have the biggest impact in catching wrongdoers and freezing and recovering assets.

Second, when the FIU / LE *does* decide to investigate a SAR, its initial intelligence may have holes in it. At the start of a case, the FIU / LE will review the intelligence provided within the SAR itself, along with any other relevant data that can be found on internal LE databases. However, due to limited FI-FI information-sharing, the SAR intelligence will often come from a single FI and is unlikely to present a high-level view of the network of accounts engaged in the suspicious activity. Without this, it can be difficult for the FIU / LE to determine which leads to focus attention on, as it does not have, for example, an understanding of where the most suspect or largest flows of money have been sent.

To rectify this knowledge gap, LE does have tools available but these can be time-consuming to use. One route is to issue a production order (PO) to an FI, which is then legally obliged to provide the requested information. However, using POs alone to piece together a web of suspicious accounts takes time: for each FI which holds relevant information, LE must request a separate PO, have the PO approved by a judge (assuming LE's request

[32] National Crime Agency, 'Submitting a Suspicious Activity Report within the Regulated Sector', page 2
[33] Maxwell, N., A Survey and Policy Discussion Paper: 'Lessons in private-private
financial information sharing to detect and disrupt crime', Future of Financial Intelligence Sharing (FFIS) research programme, July 2022, page 23
[34] https://www.fca.org.uk/news/press-releases/fca-fines-santander-uk-repeated-anti-money-laundering-failures
[35] https://www.fca.org.uk/news/press-releases/fca-fines-hsbc-bank-plc-deficient-transaction-monitoring-controls
[36] https://www.fca.org.uk/news/press-releases/natwest-fined-264.8million-anti-money-laundering-failures

meets the relevant requirements), and wait for the FI to retrieve the data from its records. This process consumes the time of LE, the courts, and FI staff, and risks slow responses to SARs, hindering LE's ability to freeze and recover any stolen assets. In addition, piecing together a network of criminal accounts in this way risks 'near misses' where LE comes close to but does not uncover suspicious links in the chain. For example, while investigating 'Criminal Account A' LE might issue a production order for the last three months of transaction data relating to this account. However, if, unbeknownst to LE, a key payment was made to 'Criminal Account B' three months and one week before the production order, LE will remain ignorant of this key connection, even after receiving the data from the FI.

An alternative route to constructing this network view of the payments and accounts linked to a SAR is to source intelligence through the Joint Money Laundering Intelligence Taskforce (JMLIT), the UK's money laundering-focused public-private partnership. Through this forum, LE can request FI intelligence, such as KYC and other data, relating to SARs or other police matters; FIs then provide on a voluntary basis. This has been a valuable tool since its inception, as it enables LE to pull in information from different FIs much more quickly than would be possible through production orders alone. Indeed, in its first five years JMLIT led to the closures of 3,400 additional accounts, the seizure or restraint of £56m in assets, and 210 arrests.[37] However, use of JMLIT is not without its challenges. FIs provide information individually and in a range of formats, and as such LE is left with the task of fitting the pieces together if it wishes to generate a high-level network view of activity. And so, while the current use of JMLIT has advantages compared to relying solely on production orders, it does not consistently enable LE to make timely interventions in ongoing money laundering cases.

The time and effort required to synthesise information from POs and JMLIT is especially challenging for the Defence Against Money Laundering (DAML) variant of SARs. As opposed to 'regular' SARs, which are submitted to the UK FIU after a suspicious transaction has taken place, DAMLs are reported by FIs or other regulated entities to the FIU when the FI / entity "has a suspicion that property they intend to deal with is in some way criminal, and that by dealing with it they risk committing one of the principal money laundering offences under the Proceeds of Crime Act 2002 (POCA)."[38] The FIU then has a statutory seven-working-day period in which to review the DAML and refuse or grant it. If the DAML is refused then the FI / entity cannot proceed with the intended business without the risk of committing a money laundering offence; they will potentially be contacted by the FIU or an LE investigation team to obtain further information for any action the FIU or LE then intends to take.[39] Given the time-pressured nature of DAMLs, the lack of cross-FI networks of data for the FIU / LE to consult puts particular strain on the system, as they only have a short window in which to gather information and make a decision.

In summary, the current AML ecosystem generates many SARs, over and above what the FIU or LE can respond to. For the SARs that the FIU or LE does choose to investigate, the processes to request FI data and piece together the network of related accounts can be lengthy. This impedes the rapid understanding of how the money laundering is taking place and where investigative resources should be targeted, inevitably reducing the FIU / LE's ability to freeze and recover assets or catch criminals. With DAMLs in particular, the FIU / LE is put under intense time pressure to piece together information.

[37] https://www.ukfinance.org.uk/news-and-insight/blogs/information-fusion-fight-against-financial-crime
[38] [39] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/167-defence-against-money-laundering-daml-faq-may-2018/file

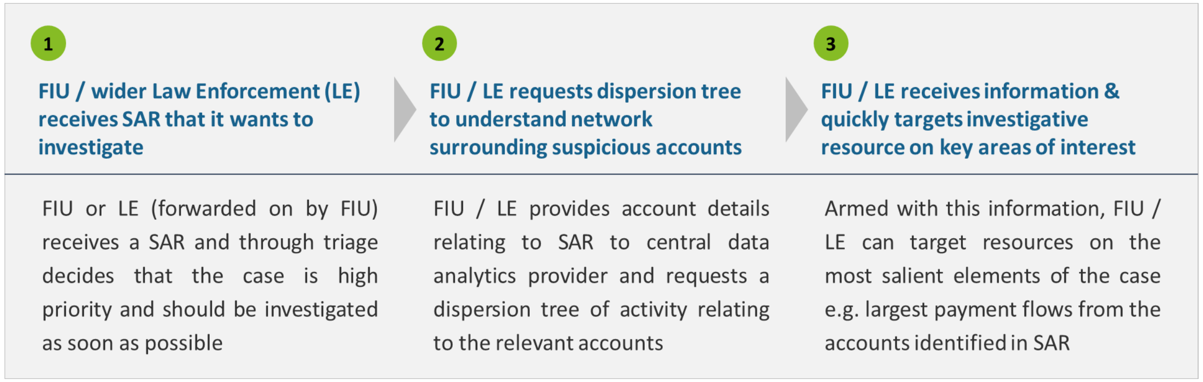
Overcoming the issue

It has been suggested by some[40] that the current SARs regime should be re-calibrated, and that the high volume of SARs submitted does not lead to effective law enforcement action. Wider conversations are required to determine what the outcomes of the AML ecosystem should be, and how to incentivise different parties – such as FIs – to ensure that they are aligned to these outcomes without fear of penalties for trying to do the right thing. These discussions of systemic AML reform, while related to the topic of this paper, are not covered here.

However, leaving that higher level concern aside, Bacs and FPS data *does* present opportunities to address the other issue outlined above i.e. that once a SAR is submitted, it is a burdensome process for LE to piece together the surrounding network of payments and accounts and then target investigations accordingly.

Approach

Figure 3 – Use Case 1



1 **FIU / wider Law Enforcement (LE) receives SAR that it wants to investigate**

FIU or LE (forwarded on by FIU) receives a SAR and through triage decides that the case is high priority and should be investigated as soon as possible

2 **FIU / LE requests dispersion tree to understand network surrounding suspicious accounts**

FIU / LE provides account details relating to SAR to central data analytics provider and requests a dispersion tree of activity relating to the relevant accounts

3 **FIU / LE receives information & quickly targets investigative resource on key areas of interest**

Armed with this information, FIU / LE can target resources on the most salient elements of the case e.g. largest payment flows from the accounts identified in SAR

For specific SARs that the FIU or wider LE wants to prioritise, the FIU / LE requests dispersion tree visualisations and supporting data based on Bacs and FPS from the data analytics provider: these visuals would depict the web of accounts connected to the suspicious activity identified in the SAR, including the scale of the different flows of money and the key accounts they have been routed through. Upon receipt of these materials and now armed with a high-level understanding of the network of accounts involved in the suspicious activity, the FIU / LE could then focus its investigation on the key accounts and bring precise requests to JMLIT or via production order to fill in any remaining gaps in information or intelligence.

This capability could equally be leveraged for LE fraud investigations, helping to identify more victims and associates of an account suspected of being used for fraud, or to indicate when the proceeds of fraud have been sent cross-border and a follow-up with SWIFT or overseas LE may be required.

Beyond economic crimes, dispersion tree visualisations could support wider LE investigations. For example, in trying to locate a suspect, an understanding of the wider network of activity around the suspect's bank account could quickly reveal their spending patterns and network of associates. Again, this could generate key leads, expanding LE's understanding of the case and ability to progress the investigation.

[40] FACTI_Panel_Report.pdf (factipanel.org)

Benefits

For the FIU and wider LE, this use case could remove significant delay from the initial investigative process in more complex cases. This would free up more time to be spent on higher value activities, leading to the more effective delivery of outcomes such as the percentage of assets frozen and recovered. Regarding efficiency, the use case could also enable LE to reduce the average length of its investigations and therefore increase the number of SARs it responds to.

For FIs, this use case could reduce the amount of time spent responding to LE requests through JMLIT or production order, due to a reduction in both the breadth and number of requests. With LE equipped with dispersion trees, it would be using production orders and JMLIT requests to fill in very specific knowledge gaps with targeted requests. This could reduce the overall number of LE requests for information, while also on average tightening the scope of each request, thereby decreasing the administrative burden on FIs in responding. A possible decrease in the number of production orders required would also save court time, which is a highly valuable resource given the backlogs currently facing the judicial system.

Technological implementation

A number of UK FIs subscribe to the MITS proposition and through it can already access FPS and Bacs-based dispersion tree visualisations, along with their supporting data. With capabilities equivalent to those MITS currently possesses and after specific details had been worked through, it could be straightforward from a technological perspective for the data analytics provider to send these products or some variation of them to LE or the FIU.

Use Case 2: Strategic assessment of impact of LE / regulatory interventions

Current AML issue

New money laundering typologies constantly emerge as criminals seek to take advantage of AML blind spots. For example, in 2018 UK LE issued warnings about the use of Vietnamese nail bars as fronts to launder proceeds from cannabis farms and prostitution, in addition to having links to modern slavery.[41] More recently, attention has turned to the cash deposit channel offered by the Post Office, through which customers can deposit cash into their bank accounts via local Post Office branches. The UK National Economic Crime Centre (NECC) estimates that "hundreds of millions [of British pounds] are laundered each year"[42] through this route.

As new typologies arise, regulators and LE respond to them and try to close loopholes. In the case of Post Office cash deposits, in April 2023 the Financial Conduct Authority (FCA) – regulator of the UK financial services industry – laid out several expectations for banks. For example, the FCA instructed that personal accounts should be limited to a maximum of £1,000 in cash deposits per 24 hours, and £10,000 in total per year. Similarly, staff should be trained in the typologies identified in Post Office cash deposits, and bank transaction monitoring capabilities should be deployed against this payment channel.[43]

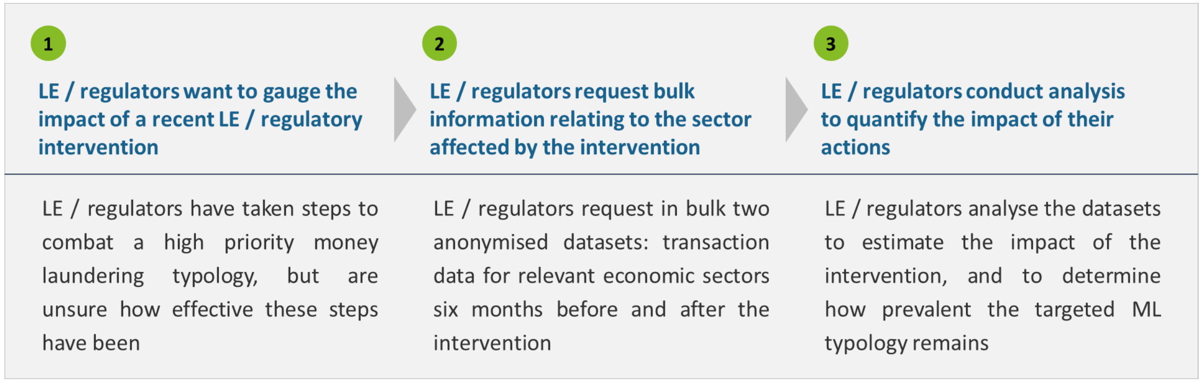
However, while LE and regulators can and do act, they lack the data to quantify the overall *impact* of their actions. The short-term effect of this is clear: the public sector can only have limited confidence that its actions have addressed the problem to be solved and may have to rely on anecdotal evidence when judging this. But in the longer term, the authorities are deprived of the ability to learn what *types* of interventions tend to be more effective in different situations, and therefore what the key levers at their disposal really are. For example, with a better feedback mechanism, LE and regulators might find that changing payment thresholds tends to be less effective, but highly targeted staff training is genuinely impactful. Such comparisons are currently not possible.

[41] https://www.theweek.co.uk/93911/nail-salons-used-as-a-front-for-modern-slavery
[42] https://www.fca.org.uk/news/press-releases/financial-watchdog-puts-banks-alert-fight-against-money-laundering-post-office
[43] https://www.fca.org.uk/firms/financial-crime/cash-based-money-laundering

Overcoming the issue

Approach

Figure 4 – Use Case 2



1 **LE / regulators want to gauge the impact of a recent LE / regulatory intervention**

LE / regulators have taken steps to combat a high priority money laundering typology, but are unsure how effective these steps have been

2 **LE / regulators request bulk information relating to the sector affected by the intervention**

LE / regulators request in bulk two anonymised datasets: transaction data for relevant economic sectors six months before and after the intervention

3 **LE / regulators conduct analysis to quantify the impact of their actions**

LE / regulators analyse the datasets to estimate the impact of the intervention, and to determine how prevalent the targeted ML typology remains

Using Bacs and FPS data, there is the potential to conduct a high-level analysis of changes that have taken place in light of LE or regulatory action. For example, if a set of policy changes were announced on date X to address a problem, after an intervening period LE or the regulator could request data relating to the specific sector of the economy that was targeted, receiving cuts from the six months preceding and following date X. To avoid unnecessary exposure of personal information, these cuts could be anonymised, albeit with appropriate tagging to allow for meaningful analysis.

So, if assessing the impact of interventions against nail bar-centred money laundering, LE would provide information to the data analytics provider identifying nail bar accounts. The data analytics provider would then create a full dataset of transactions taking place to and from these accounts, in addition to transactions from accounts a specified distance up and downstream of the nail bar accounts.

If deemed necessary, this data could be anonymised and reported to LE in a form where nail bar accounts are not specifically identified but labelled as ‘Nail Bar 1’, ‘Nail Bar 2’ or equivalent, and with non-nail bar accounts fully anonymised. These two ‘before’ and ‘after’ datasets could then be sent for analysis to the NECC within the NCA or another appropriate public sector body. Alternatively, if LE judged it lacked the capability or capacity to conduct the analysis itself, it could contract with the data analytics provider or another third party to do so on its behalf.

Following analysis, findings could be shared with FIs so they would also have visibility of the intervention’s effect on payment flows. FIs could add to this any qualitative observations (e.g. complaints from customers about constraints the intervention places on the usage of their accounts) they had made during the period, broadening the conversation so the intervention could be judged in the round.

When conducting this strategic analysis, it is possible that the analyser (whether NECC, another public sector body or a private sector party) could uncover at a tactical level certain networks of payments that remain highly suspicious in the ‘after’ dataset. In such situations, LE or the regulator could request that the data analytics provider de-anonymise the relevant account information so a full investigation could proceed.

Benefits

The benefits for LE and regulators arising from this use case are clear. At the strategic level, it would enable these public sector bodies to understand the impact of their interventions and thereby more closely determine whether further action is necessary; this would lead to a more effective system-wide response to money laundering, with loopholes closed more definitively once identified. Over the longer term, it would hone the public sector's understanding of the key levers at its disposal, as well as generating tactical intelligence into any outstanding pockets of the typology that have not been disrupted by previous interventions.

While noting the benefits above, it is important to caveat the limits of analysis based on this dataset. First, while 'before' and 'after' data cuts may highlight changes in payment patterns either side of an LE or regulatory intervention, that would not guarantee that those changes are the result of the intervention alone; other factors would also need to be considered. Second, attention would need to be paid to the unintended consequences of an intervention. These might not be captured within the patterns of transactional data but would still be important in assessing the intervention's overall effectiveness.

FIs would also reap several benefits from the use case. LE / regulator-led strategic-level analysis, once shared with FIs, would increase FI understanding of the nature of the typology being addressed and the public sector-led response to it. First, this might enable FIs to finetune their controls to the threat, given the extra detail they are provided with by the public sector. Second, exposure to this 'before' and 'after' analysis would improve FI confidence in the proportionality and effectiveness of the measures encouraged or mandated by the public sector. This could have positive knock-on effects for any measure's ongoing implementation within FIs as well as for staff buy-in – AML practitioners would be motivated when shown the impact that new or altered procedures are having. And third, the sharing of this analysis would keep the dialogue between FIs, LE and regulators open, putting FIs in a stronger and more informed position to voice their own recommendations for interventions as each new high-priority typology is identified.

Technological implementation

Technologically, while Vocalink does not provide sector-specific, anonymised six-month transaction data cuts to FIs currently, the generation of these products relies on the same underlying capability it uses to produce dispersion tree visualisations – namely, tracing the flow of payments between different accounts. The exact details of the output required by LE would need to be agreed but, whatever those requirements were, a data analytics provider with capabilities to the level that Vocalink currently holds should be able to adapt to them.

Use Case 3: Leveraging MITS capability to monitor for a specific ML typology

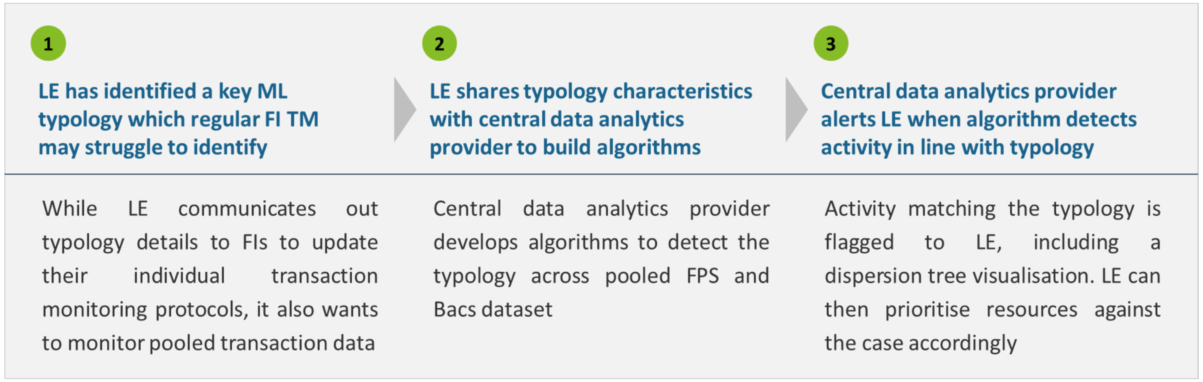
The issue

As noted in the discussion of Use Case 1, it is difficult for FIs, monitoring transactions relating to their own accounts alone, to detect complex money laundering networks that run across multiple institutions. It would be more effective to apply AML algorithms to a dataset from multiple FIs, but this has not yet been achieved at scale in the UK. In addition, money laundering typologies are constantly evolving, and as each new typology is 'invented' by criminals, it takes time for the system to catch up. First the typology must be recognised by LE or an FI, then its existence communicated out to all FIs, and finally FIs must design and implement appropriate monitoring policies. Any reduction in the delay between identifying a typology and monitoring for it at scale across the financial system therefore holds the potential to detect criminals sooner and limit the value of money laundered.

Overcoming the issue

Approach

Figure 5 – Use Case 3



1. **LE has identified a key ML typology which regular FI TM may struggle to identify**

While LE communicates out typology details to FIs to update their individual transaction monitoring protocols, it also wants to monitor pooled transaction data

2. **LE shares typology characteristics with central data analytics provider to build algorithms**

Central data analytics provider develops algorithms to detect the typology across pooled FPS and Bacs dataset

3. **Central data analytics provider alerts LE when algorithm detects activity in line with typology**

Activity matching the typology is flagged to LE, including a dispersion tree visualisation. LE can then prioritise resources against the case accordingly

In a case where LE has discovered a new money laundering (or fraud) typology which (1) it considers a high priority for disruption, and (2) will be particularly challenging for siloed FI transaction monitoring systems to detect, LE shares typology details with the data analytics provider. The provider then designs and implements algorithms bespoke to the typology, sharing alerts with LE. Individual FIs would still be requested to update their own monitoring approach as another line of defence against this new threat.

As well as passing information regarding known new typologies to the data analytics provider, there is a possible variation to this use case where the provider analyses payments data in bulk to identify unknown unknowns, i.e. new typologies which LE and individual FI transaction monitoring processes have not previously identified. When such examples are found, the provider could build algorithms to detect them within Bacs and FPS transactions, as well as sharing details with FIs to update their own monitoring systems. The effectiveness of this variation could be amplified by clashing pooled payments data with confirmed LE intelligence. The National Data Exploitation Centre (via the NECC) could be an important potential partner in this context.

Benefits

Regarding benefits for LE, first it would have access to a transaction monitoring system with the potential for highly effective detection, given its use of payment data from across multiple institutions. LE could therefore receive a stream of highly relevant, high priority SARs from the provider, and, if combined with Use Case 1, the network-level representations of accounts relating to each SAR to enable swift investigative follow up. Second, it would be able to mobilise this method of detection faster than could be achieved by waiting for each FI to update its own transaction monitoring procedures: for Use Case 3, the typology only needs to be understood and algorithms implemented once by the data analytics provider for system-wide detection to be in place; without Use Case 3, this needs to be done by every individual FI to achieve the same level of coverage. For the same reason, Use Case 3 would also allow for faster system-wide upgrades to algorithms as understanding of different typologies increases, with updates needing to be made in one place alone rather than across a range of actors.

There are benefits for FIs too. As FIs look to update their own transaction monitoring processes against the typology, they would be able to draw on insight from the data analytics provider's approach to finetune their own algorithms. Furthermore, in the longer-term this use case would build up learning about, and evidence for the efficacy of, more centralised approaches to transaction monitoring. This could ultimately present opportunities for the consolidation of transaction monitoring into a central utility, significantly reducing costs among FIs who could reduce the scale of their internal operations while sharing the cost of the central mechanism between them.

Technological implementation

Through the MITS proposition, algorithms are applied to monitor Bacs and Faster Payments data and identify suspected mule accounts, alerting FIs when these accounts are held by their customers. Currently these algorithms are geared towards the detection of money mule activity; however, for an analytics provider with MITS' existing level of capability in place, it would be possible to build in new algorithms to detect other emerging ML typologies too.

Potentially the biggest challenge to overcome would be in translating LE's understanding of a new typology into a form that could be encoded into an algorithm or digital typology: LE may be more likely to view typologies through the lens of observable phenomena, such as the types of business involved or key websites; a new transaction monitoring algorithm, on the other hand, would need to be programmed with the payments patterns that accompany these phenomena. For this use case to work, once LE has identified (or been informed of) a new typology, it or a supporting third party would need to collect information on the payment patterns that were associated with the criminal activity and then express this to the data analytics provider's data scientists to encode.

This would require access to people with the right skills, and so as with Use Case 2, it may rely on LE to invest to build capability internally or pay or partner to secure it from a third party.

If this use case were piloted, it would be important to assess the extent to which effective typology detection is restricted by the lack of contextual data on accountholders held within FPS and Bacs transaction data. FI transaction monitoring incorporates KYC information into its assessment of an account's transaction patterns before generating alerts; the process described in this use case, however, would not have access to this type of contextual data. Evidence generated in a pilot would help to test whether the advantages from monitoring transactions across multiple FIs would be enough to lead to effective detection, even without the support of contextual account information.

Obstacles to delivery

Feedback suggests the use cases above are technologically feasible. However, there are potential obstacles in securing funding and FI permissions before these use cases can be mobilised.

Commercial obstacles

The three use cases do require some additional functionality beyond existing capabilities which would require financial support to develop.,. Furthermore, as noted above, LE might require internal investment or external support to analyse the anonymised payments data that it receives for Use Case 2 and to 'translate' LE-observed typologies into encodable patterns of transactions for Use Case 3. The time and effort required for these things would have cost implications. While commercial discussions would need to be held for the data analytics provider, LE and any other relevant parties to determine where costs would fall, there are emerging sources of public sector funding which could be used to support any regulatory or LE cost obligations.

Firstly, funds might become available through the Economic Crime Levy which has been introduced this year. An annual charge affecting entities which are supervised under the Money Laundering Regulations (MLR) and whose UK revenue exceeds £10.2 million per year,[44] the levy is expected to raise £100 million per annum.[45] Over £100 million of this has been allocated for investment into "state of the art technology which will analyse and share data on threats in real time" over the next three years,[46] and might therefore be available for use in payments architecture-based solutions.

[44] https://researchbriefings.files.parliament.uk/documents/CBP-9380/CBP-9380.pdf, page 4

[45] *Ibid.*, page 1

[46] https://hansard.parliament.uk/commons/2023-03-27/debates/23032711000010/EconomicCrimeLevyAllocationsUpdate

Secondly, increased funding might become available through the Asset Recovery Incentivisation Scheme (ARIS). The ARIS was launched in 2006 and allocates to law enforcement 50% of the money they recover, following any cost deductions and contributions to the separate ARIS top slice fund, used to support key national asset recovery capabilities. The ARIS distributions to LE agencies in 2021-22 rose by 60% compared to the year before to a figure of £142 million,[47] while top slice funding – used to fund key national asset recovery capabilities – rose to £13.9m.[48] If initial investment can be found to support more effective, information sharing-based responses to economic crime which result in better asset recovery outcomes, there is the prospect of greater future investment from the ARIS through direct distributions or the top slice as LE settles into a virtuous cycle of recovering more and then being able to spend more.

Thirdly, a High Court case heard in November 2022 opens up the prospect of a new funding stream. In what has been called the first case of its kind, the NCA obtained a civil recovery order to take control of £53.9 million of funds from 30,000 former account holders of an FI. The FI had previously frozen these funds after identifying in 2011 that they potentially represented the proceeds of unlawful conduct.[49] It is not yet clear how this money will be spent. However, some of it could be allocated as a strategic investment in information-sharing initiatives.

Furthermore, now that the precedent has been set, additional funds may become available if equivalent cases are brought and meet success over the coming years.

In summary, while the use cases will come with costs, there are potential sources of funding – but they need to be prioritised against this opportunity.

It should also be noted that, depending on choices made during implementation, the pursuit of these use cases could be in relative terms a high potential, low cost, and low risk investment. The high potential of these use cases has been discussed above. In terms of cost, building capabilities where data is already aggregated means the funds required would be significantly lower than those needed to develop a similarly capable, greenfield utility. Finally, the risks should also be lower as LE could easily stop pursuing these use cases if they proved ineffective: LE would not have made significant investments in a new platform and therefore would not feel the pressure to continue a failing project to justify previous sunk costs; and the provider would also be relatively lightly affected, for example with the MITS proposition being able to continue to serve subscribing FIs regardless of whether LE were involved or not.

Of course, proceeding with a different data analytics provider would come with a different array of strengths and weaknesses which may overall prove more attractive to LE; this paper, as previously mentioned, does not seek to express a view on that decision.

Legal and permission-based obstacles

A potentially challenging obstacle to overcome may be in securing FI permissions for the use cases to go ahead. While Vocalink operates the Bacs and Faster Payments systems on Pay.UK's behalf, the data is owned by the FIs to whom customer accounts belong. As such, the existing MITS capability operates only because the FIs that subscribe to it have authorised their data to be used in its processes. Since each of the proposed use cases would constitute a material change to these processes, they would require a renewal of FI permissions. Relatedly, MITS reports only use information from FIs signed up to its service, not all those linked to the Bacs and FPS systems. This limits the overall dataset that the use cases would draw upon; their impact would be increased if all FPS and Bacs data could be brought into scope. Again, permission would be required for this from the relevant FIs.

[47] https://www.gov.uk/government/statistics/asset-recovery-statistical-bulletin-financial-years-ending-2017-to-2022/asset-recovery-statistical-bulletin-financial-years-ending-2017-to-2022#use-of-asset-recovery-incentivisation-scheme-aris-funds

[48] https://questions-statements.parliament.uk/written-questions/detail/2022-01-04/96901

[49] https://www.33knowledge.com/latest-news/civil-recovery-of-significant-funds-held-across-thousands-of-accounts-at-uk-bank

There are three high-level routes that could be taken to secure these permissions. First, LE, Pay.UK, the Payment Systems Regulator (PSR) and FIs could come together to discuss the use cases and collectively address any concerns. As the NCA is the ultimate recipient of data arising from the use cases, Section 7 of the Crime and Courts Act 2013 could be assessed as the potential legal information gateway to enable FIs to navigate their confidentiality obligations to customers: subsection 1 states that "A person may disclose information to the NCA if the disclosure is made for the purposes of the exercise of any NCA function"; subsection 8 adds that "A disclosure of information which is authorised or required by this Part does not breach (a) an obligation of confidence owed by the person making the disclosure, or (b) any other restriction on the disclosure of information (however imposed)."

Data protection concerns would also need to be addressed. The parties would need to determine to what extent these will have been eased once the Data Protection and Digital Information Bill comes into law (at the time of writing, it is passing through the UK Parliament). The bill "gives more confidence to organisations to rely on the legitimate interests lawful basis [in UK GDPR] and to further process data", setting out "'recognised legitimate interests' where no balancing test is required"[50] before data processing can take place. One of these recognised legitimate interest's is in instances when "[data processing] is necessary for the purposes of – (a) detecting, investigating or preventing crime, or (b) apprehending or prosecuting offenders",[51] and therefore may well be applicable to the proposed use cases. Second, if an agreement cannot be reached between parties for information sharing to take place voluntarily, LE and the PSR could look to compel sharing through existing powers. For example, the PSR may be able to use its Section 54 powers under the Financial Services (Banking Reform) Act 2013, through which it can "require or prohibit the taking of specified action in relation to the system" by participants in regulated payments systems.

Third, if existing powers are not sufficient, the government could be called upon to pass specific enabling legislation.

Each of these approaches come with different benefits and drawbacks. LE and regulators may wish, in the first instance, to proceed with a more collaborative approach building on existing legal gateways; Compelling sharing, on the other hand, could lead to quicker implementation and would provide the highest assurance to FIs that information could be legally shared, but the passage of new legislation would take time delaying when the use cases could first be implemented and could also impact goodwill among FIs.

However, it is important to note that while the use cases could have significant impacts, they reflect a limited extension on activity that is already taking place through the MITS proposition. In Use Case 1, dispersion tree reports – which MITS already produces – would be sent to LE rather than just FIs as currently, and only to support active LE investigations. In Use Case 2, while the use of FI data departs from the existing MITS proposition, the data could be anonymised. In Use Case 3, MITS' *existing* core capability of monitoring FPS and Bacs data acts as the foundation; the extension of the proposition is simply in using this capability to monitor for additional, LE-defined typologies, and reporting alerts back to LE. These use cases are intentionally restrained in the extent to which they would require the data analytics provider to depart from what already occurs.

Additionally, it should also be noted that centralised analytics already takes place in relation to card data, and that payments data is already analysed by FIs (for example to detect fraud) but is done so in silos. The use cases set out here, simply extend that same analysis at a collective level but also make it intelligence led, which would help reduce collateral intrusion on the right to privacy by enabling analysis to be significantly more focussed.

Given the potential benefits they could bring to the fight against economic crime, the ideal aim would be for their approval through mutual agreement by all parties once any contentious details (such as how data might be controlled once shared) have been addressed.

One final reflection is around the higher-level implications these use cases may have regarding the role of the private and public sectors in the UK

[50] https://ico.org.uk/media/about-the-ico/consultation-responses/4025316/response-to-dpdi-bill-20230530.pdf
[51] Data Protection and Digital Information Bill, Schedule 1 Paragraph 5, as copied on 17th July 2023 (https://bills.parliament.uk/bills/3322)

AML regime. Use Case 3 in particular, would see LE encroaching into the field of transaction monitoring which has historically been the domain of FIs, and would create a system of duplicated transaction monitoring where FIs and LE (via the data analytics provider) might both be monitoring for the same typologies. This raises long-term questions, such as whether ultimately FIs could be relieved of their individual transaction monitoring duties as these move to a centralised utility – a change which could help reduce FI compliance costs. As information-sharing utilities become more embedded into the UK's AML ecosystem, the answers to such questions may become clearer. For now, the proposals in this paper would purely be additional to existing AML activities.

In summary, across these use cases, collective analysis of FPS and Bacs data offers clear opportunities to increase LE and regulator responses to money laundering, fraud, and other crime at an operational, tactical, and strategic level. Encouragingly, the technological difficulty of implementing these use cases appears modest, and there are possible sources of funding available to help address cost implications. The most significant obstacle may be in testing legal gateways and securing agreement from FIs for their data to be used in these new ways. FIs' obligations of confidentiality to their customers and their risks of liability are important and must be respected. However, through clear dialogue between LE, regulators and the FIs, there may be the chance for all parties to agree a route forward in the current legal framework.

It is also important to note that these use cases can be taken forward individually. This would allow parties, if needed, to grow in confidence by first trialling the use case that is perceived to pose the lowest legal risk, laying the foundation for the other use cases to be implemented in time.

Next steps

As a first priority, stakeholders from LE, Pay.UK, the FIs and other key stakeholders would convene to discuss the use cases presented here in addition to any other suggestions that draw on FPS and Bacs transaction data. This forum could be used to develop and share the possible benefits and drawbacks each type of stakeholder will be exposed to by the different use cases, creating a common understanding among stakeholders about the key issues. This forum should also consider the most effective mechanism to create a mechanism that allows for healthy competition between analytics provides to support the development of the use cases.

From these initial insights, the parties should aim to select the priority use cases they want to take forward in the immediate term and agree the key commercial and legal milestones needed to achieve unanimous approval to proceed with a pilot and should also consider the process they will use to move from pilot to full use case mobilisation, assuming the pilot is effective.

In tandem, and in line with ECP2 Action 33 to strengthen its role as leader of the economic crime system, the NECC could coordinate with the data analytics provider to explore the opportunities for public sector analysts to temporarily second into the provider and gain hands-on experience of the payments data and analytical capabilities that can be applied to it. This would help to build skills within the public sector and further its awareness of the additional public interest use cases which the data could be used to create.

4: Opportunities in the New Payments Architecture

While more can be done with data within the payments infrastructure today, the UK's New Payments Architecture (NPA) programme, overseen by Pay.UK, could make the use cases in this paper yet more effective in future. First conceived in 2015,[52] the programme will build the UK's next generation retail payments infrastructure, with Faster Payments and then Bacs (subject to industry consultation) to move onto the new system.[53] A supplier will have been chosen to deliver the NPA by the end of summer 2023, with full implementation to follow by June 2026.[54] Particularly in the adoption of the ISO 20022 messaging standard, the promise of overlay services, and the wider context of change its implementation will create among FIs and other stakeholders, the NPA is rich with opportunity for the use of payments data to combat economic crime.

ISO 20022

One of the six guiding principles of the NPA is the "Adoption of the ISO 20022 messaging standard, which will enable new capability, for example tracking and tracing payments". Once in place, ISO 20022 will see transaction data become more standardised. It will also bring in enhanced data fields which have not previously been captured and which in some cases may be made compulsory by regulators over time. For example, as the Bank of England oversees the adoption of ISO 20022 in the UK's CHAPS high-value payments rail, it is *encouraging* the use of purpose codes, documenting the intent of a payment, from June 2023, before *mandating* them for FI-FI and property payments from November 2024.[55] Other examples of enhanced ISO 20022 data are structured remittance data, structured addresses, and legal entity identifier numbers, all of which will in time enrich the pool of data available for analysis.

Reflecting on this potential, UK Finance has observed that sanctions screening will be significantly improved, compared to the current system which relies on fields that "[contain] shortened and often inaccurate data." Similarly, for transaction monitoring, "[a]ccessing more complete payment fields will improve the identification of typologies".[56]

Furthermore, ISO 20022 comes with the promise of greater interoperability as it can act as a bridge, allowing the same fields within different data standards to be mapped more easily to one another. It is also being adopted worldwide: NatWest has predicted that by 2026, 80% of high-value domestic payments by volume (and 90% by value) will take place using ISO 20022, and that the standard will be adopted in more than 50 countries.[57]

[52] https://www.psr.org.uk/our-work/new-payments-architecture-npa/
[53] https://www.wearepay.uk/programmes/new-payments-architecture-programme/
[54] https://www.finextra.com/blogposting/24078/new-payments-architecture-infrastructure-must-drive-innovation-and-reduce-costs
[55] https://www.bankofengland.co.uk/-/media/boe/files/payments/rtgs-renewal-programme/iso-20022/policy-statement-implementing-iso-20022-enhanced-data-in-chaps-january-2022.pdf
[56] https://www.ukfinance.org.uk/news-and-insight/blog/making-most-iso-20022-help-tackle-financial-crime-compliance
[57] https://www.natwest.com/corporates/insights/regulation/more-than-just-a-messaging-system-the-benefits-of-iso-20022-and-how-to-approach-its-adoption.html

This common data standard increases the technological prospect of international information-sharing and traceability of payments to combat money laundering, although legal and commercial considerations will also need to be addressed.

Overlay services

Another key NPA feature which will support anti-economic crime use cases is the development of overlay services. In essence, third parties will be able to develop and sell additional services which, with the approval of Pay.UK, draw on NPA data to offer functionality beyond the NPA's core capability of processing payments. An early overlay service that has been developed is Confirmation of Payee (CoP). This informs a payer whether the payment details they have entered for a payee correspond to those held by the payee's service provider, indicating whether the details are a match, a close match (e.g. "Joseph Bloggs" instead of "Joe Bloggs"), or do not match. In this way, CoP enables payers to avoid loss of funds through accidentally misdirected payments, while also mitigating the risks of certain types of fraud. In October 2022, the PSR made it a requirement for Payment Service Providers (PSPs) connected to the Faster Payments network to provide CoP to their customers.[58] Pay.UK followed up on this, announcing that they have been "informed by a number of firms that they are developing or have developed technical solutions for [Payment Service Providers] wishing to adopt the Confirmation of Payee service. Any [Payment Service Provider] wishing to know the names of these solution providers or any firm wishing to be included on the list is welcome to contact us for this purpose."[59]

While uncertainty remains around exactly how the NPA will be implemented and the limits this – along with further legal and commercial considerations – may place on the types of overlay services which will be provided (promisingly, Pay.UK has already announced the development of a fraud overlay service),[60] CoP offers a positive model for the development of anti-economic crime solutions in the future. If the NPA can act as an open environment which actively encourages different third parties to leverage its underlying data, it could prompt the release of a range of innovative services which FIs and LE might not have had the capacity or capability to architect themselves.

In addition, where the regulator (as has happened with CoP) *requires* FIs to adopt certain services, FIs will be more likely to have a range of potential providers to engage and thereby a better chance of accessing a good solution at a competitive price. To fully realise this potential, it is critical that the proliferation of different overlay service providers does not in effect recreate data siloes – Pay.UK should aspire to deliver a system where FIs subscribed to different economic crime overlay service providers can still receive a service which leverages each other's data.

A context of change

A final opportunity presented by the NPA is that the process of its implementation will create a context of change. While the adoption of the use cases proposed in this paper in the immediate term would represent a previously unadvertised departure from the status quo, FIs and other payment service providers know that the NPA programme will be making changes over the next few years; as such, during this transition period they may be more open to taking any further steps required for these use cases given that many other policies and processes will be evolving.

In summary, through the adoption of the ISO 20022 standard, the creation of overlay services, and simply the wider context of change that its implementation will foment, the NPA provides a significant opportunity for the mobilisation of the use cases proposed in this paper as well as further solutions. However, it is essential that stakeholders from the anti-economic crime sector are engaged through the NPA's design and construction, so that the potential of this moment is not wasted. Indeed, it is critical (both in the UK and globally) that tackling economic crime is made a key consideration in the development of new payments systems and the implementation of ISO 20022.

[58] https://www.psr.org.uk/media/zxgkagpj/psr-specific-direction-17-expanding-confirmation-of-payee-oct-2022.pdf

[59] https://www.wearepay.uk/what-we-do/overlay-services/confirmation-of-payee/

[60] https://newseventsinsights.wearepay.uk/media-centre/press-releases/payuk-partners-with-visa-synectics-solutions-and-featurespace-on-pioneering-fraud-detection-and-prevention-initiative/

5: An overarching strategy for UK information-sharing utilities

To reach the full potential of the use cases laid out in this paper - both at present and once the NPA is rolled out - it is important that, if adopted, they are placed within an ordered information-sharing movement which is strengthened rather than fragmented as new utilities are constructed. A number of other information-sharing solutions have been or are being piloted in the UK. For example, the Tri-Bank pilot pooled transactional data from three banks in pseudonymised form to reveal suspicious patterns of activity;[61] the Public Sector Fraud Authority within the Cabinet Office is developing a “Single Network Analytics Platform for cross-government/and UK banking sector use”;[62] and Pay.UK has described its work on an Enhanced Fraud Data Standard as the latest stage in its “ambition of building an Application Programming Interface (API) solution through which standardised customer data will be sent”, ultimately to help identify suspicious payments or Authorised Push Payment (APP) scams before funds are transferred.[63] This volume of activity is encouraging, but must be directed by a coherent, overarching strategy. In Singapore, for example, the Monetary Authority of Singapore is leading the development of the COSMIC utility and providing a clear vision for how information-sharing will be taken forward. This likely increases private sector confidence in the direction of travel and the long-term value of any investment they make.

Fortunately, the release of ECP2 has signalled the UK government’s intent to provide equivalent leadership through a new public-private economic crime data strategy which will “enhance the exploitation of available data across the ecosystem to better prevent, detect, and pursue economic crime.”[64] This section outlines some key considerations this strategy should seek to address.

Overarching objectives

It is a key enabler for the data strategy that the overarching UK anti-economic crime objectives it will support are clearly defined. Research surveys conducted in this field have previously noted that a number of policy questions will need to be addressed as information-sharing augments system-wide anti-economic crime capabilities. For example, AML policy in time will need to have “a clear position as to whether financial exclusion for high-risk entities is desirable and intended or not.”[65] The sooner these types of question can be answered, the better-equipped the data strategy will be able to shape the capabilities required to support the government’s overall vision for the sector.

[61] https://www2.deloitte.com/uk/en/blog/economic-crime/2022/utilities-an-important-tool-in-fighting-financial-crime.html
[62] https://www.globalgovernmentfintech.com/uks-public-sector-fraud-authority-turns-to-cutting-edge-tech/
[63] https://newseventsinsights.wearepay.uk/media-centre/press-releases/payuk-and-uk-finance-publish-first-iteration-of-technical-collateral-for-enhanced-fraud-data-standard/
[64] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1147515/6.8300_HO_Economic_Crime_Plan_2_v6_Web.pdf
[65] Maxwell, N., A Survey and Policy Discussion Paper: ‘Lessons in private-private
financial information sharing to detect and disrupt crime’, Future of Financial Intelligence Sharing (FFIS)
research programme, July 2022, page 76

Preventing siloes

One feature that should be prioritised by the strategy is in ensuring the breadth of data coverage offered by utilities: the greater the pool of data available for sharing, the greater the potential anti-economic crime benefit. If different utilities emerge which offer the same function but to different groups of FI participants, and they are unable to communicate with one another - key data will still be siloed; the ideal end-state is the availability of information sharing across all relevant actors. There are different ways to achieve this, for example, by the public sector ensuring that rival utilities do not emerge and fragment information between them, or by allowing the creation of competing utilities but setting clear interoperability requirements so that data siloes are not created. If the right decisions are taken during its implementation, the NPA offers another potential model, combining a centrally managed infrastructure and pool of data with an array of third parties able to develop and offer competing overlay services based upon it. This strikes a balance between preventing data siloes but enabling competition.

It is important too to prevent silo-ing between different economic crime domains. Any barriers between, for example, information used to tackle money laundering and fraud should be avoided unless absolutely necessary.

Laying the groundwork for international information-sharing

Beyond information-sharing within the UK, the data strategy should address how it will lay the foundations for the future possibility of increased international sharing. Criminals commit economic crimes across borders, and the arguments made for information sharing at a domestic level equally apply internationally. As well as exploring the option of international information-sharing pilots, the strategy should ensure time is spent evaluating the sufficiency of the UK's existing legislation to enable international sharing. It should also reflect on how the UK should determine what and how prominent a position it wants to take in the face of current "trends towards more restrictiveness"[66] in data localisation measures, which could impede the international information-sharing agenda.

Looking beyond traditional financial data

Another key element to the strategy will be in enabling information sharing beyond the traditional financial system. Criminals will constantly test the financial system to locate vulnerabilities.

As information sharing of FI data increases, it may succeed in reducing economic crime through one part of the financial system only for it to be displaced into others, unless the scope of data to be shared can evolve and continue to eliminate black spots. This will be a constant challenge as different payments methods and economic crime techniques evolve, some of which may sit outside the immediate domain of FIs.

One emerging area of risk is cryptocurrencies. Blockchain analysis of "on-chain" crime, i.e. where the assets stolen or otherwise acquired by criminals were held as cryptocurrencies at the moment they came into criminal possession – estimates that $23.8 billion worth of cryptocurrency was laundered in 2022, with just under half of this sum sent to mainstream, centralised crypto exchanges which can act as "fiat off-ramps, where the illicit cryptocurrency can be converted into cash."[67] Laundering is also operating in the opposite direction – from illicit cash into crypto – with the NCA's National Assessment Centre estimating that "likely over £1 billion of illicit cash is transferred overseas using cryptoassets" and "hundreds of millions of pounds are likely laundered via over-the-counter crypto brokers".[68]

[66] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1125805/Frontier_Economics_-_data_localisation_report_-_June_2022.pdf
[67] Chainalysis, 'The 2023 Crypto Crime Report', February 2023, pages 42-3
[68] https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-cryptoassets-technical

Indeed, the NECC's director has observed in interview that the proportion of money laundering done through crypto, while relatively low, is expected to increase rapidly and supports international criminal networks to an unprecedented scale.[69]

Another field for attention is engagement with tech and social media companies. There is a perception among UK FIs that social media companies for example, need to do more to prevent the origination of fraud on their platforms. Following the launch of the UK's Fraud Strategy in May 2023, nine UK FI CEOs wrote to the Prime Minister questioning the likely effectiveness of a strategy that "fails to mandate action on all actors involved in the fraud journey".[70] Relatedly, other commentators have observed that "The measures advocated in the strategy to reduce the outsized role played by social media and tech companies in facilitating fraud and scams are voluntary and do not go far enough."[71]

The data strategy needs to determine how it will build links to these important data sources now, as well as considering how the system can set itself up in the long-term to be nimble in leveraging other data sources as they gain value due to shifts in criminal practice.

Balancing privacy and effectiveness

The strategy should also determine how it balances the effectiveness of information sharing against the need for data protection and confidentiality. As can be seen through the different pilots that have already taken place, utilities can be constructed in different ways to address different problems. As these approaches are tested further, there will be a greater understanding of how effective each variant is and the degree of personal data it relies upon. The strategy should ensure there is a mechanism in place to continually assess these findings and use them to build and maintain a system of utilities that is as efficient in its use of personal data as it is effective in detecting economic crime. In addition, a clear process must be in place for the effective imposition, monitoring and update of data security requirements over time.

These steps will not only limit the risks posed through data breaches or insider threats but will also help to build public consent for information sharing.

Harnessing competition and innovation

As mentioned above, it is important that the strategy provides an overarching structure for new utilities as they emerge; for example, clear interoperability requirements should be signalled to prevent utilities from themselves becoming siloes. However, it is important for the strategy to achieve this in a way that does not restrict the positive forces of competition and innovation. The Privacy Enhancing Technology (PET) Prize Challenges, set up by Innovation UK and the US Centre for Data Ethics and Innovation in June 2022,[72] illustrate how a central authority can use structured contests to drive innovation in selected areas.[73] The NPA's approach to overlay services shows another way that the public sector could promote innovation, by centrally identifying a required service which different suppliers can then compete to design and market to end users, based on a centrally provided data source. The data strategy should look to leverage these or similar mechanisms to create the conditions for well-directed, high-value private sector competition and innovation.

[69] https://www.ft.com/content/83b5932f-df6f-47a6-bf39-aa0c3172a098
[70] https://news.sky.com/story/bank-chiefs-tell-sunak-to-make-big-tech-bear-cost-of-fraud-pandemic-12904163
[71] https://rusi.org/news-and-comment/rusi-news/rusi-experts-react-uk-governments-new-fraud-strategy
[72] https://www.ukri.org/blog/privacy-enhancing-technologies-pets-prize-challenges-winners
[73] https://petsprizechallenges.com/

In whatever way the strategy harnesses the powers of innovation, it should also strike the balance between 'quick wins' and long-term potential. It is important that information-sharing practices realise value in the short-term to build momentum and thereby maintain or increase public and private investment in the area. However, time is also needed to develop critical infrastructure, such as the NPA, that is robust and flexible enough to support different use cases as they emerge in the longer term. The use cases presented in this paper offer solutions that should be technically achievable and could be mobilised quickly once legal concerns are resolved. A well-balanced portfolio of work within a national strategy could include this type of opportunity, as well as longer-term initiatives presented by the NPA and the Cabinet Office's Single Network Analytics Platform. It would also explain how these separate strands would coherently come together once all in place.

In summary, there are several, often interdependent, considerations that the data strategy will need to address. It is essential, if it intends to maximise the possible benefits from information sharing, that it focuses on reducing information siloes, most immediately between domestic FIs, but also in the longer term across borders and beyond the traditional financial system. Data privacy concerns must be embedded throughout, and competition used to drive private sector innovation. The strategy does not need to fully address all these issues now, but it should at least demonstrate the overarching process and enabling conditions it will create to see that they are addressed in time. For example, it might not be realistic for the strategy to lay out in detail exactly what types of utility the UK requires and what capabilities they should offer; however, it *can* explain how it expects the government to develop its position on this, and which organisation(s) will be responsible.

6: Conclusion

The anti-economic crime landscape is currently in a phase of active experimentation with information-sharing approaches to combat money laundering and other crimes; this is encouraging, and the success of any one jurisdiction in creating a utility will provide learning for the benefit of all. Some of the most visible developments in the field, exemplified by COSMIC and TMNL, have revolved around building a greenfield information-sharing platform to address specific use cases. This has clear advantages, primarily that the construction of the utility can be shaped precisely to the use cases it is intended to serve now and may expand to serve in future. The utility can be set up for long-term success.

Yet, given the urgency of addressing global money laundering, fraud, and wider economic crime threats, there are opportunities that may allow some of the benefits of information sharing to be realised in the much shorter term. Significant time and cost are incurred in creating a utility to pool financial data, and so it is important to assess the potential of those parts of the financial system where such data is already pooled.

To that end, this paper has focused on the UK and how data from the Bacs and FPS payment rails could be used to address particular issues in law enforcement and regulators' response to money laundering and fraud. While these proposed use cases are technologically straightforward, there are commercial and legal obstacles that will need to be addressed. To do this, we recommend that stakeholders from LE, Pay.UK, Vocalink / an alternative analytics provider and the FIs convene to discuss such use cases and to define the commercial, legal, and other milestones that need to be reached for pilots and full mobilisation to be achieved. Equally, the NECC and the chosen analytics provider should explore the opportunities for selected public sector analysts to temporarily second into the provider and gain hands-on experience of its capabilities and the data it uses.

Looking beyond the UK, the arguments made here should validity in other jurisdictions. That is, other jurisdictions are likely to have similar points of data aggregation in their payments architecture too, and specific use cases this data could be used to support. We urge policymakers worldwide to identify these points in their own financial systems and to start the conversation between government, law enforcement, regulators, payment system operators and FIs as to how they could be leveraged. The construction of next-generation payment systems and the adoption of ISO 20022 makes such conversations particularly timely, as the data standard can enhance the potential of payments data to combat crime. However, this potential is unlikely to be realised on its own, and anti-economic crime professionals and policy makers (both domestically and globally) should work now to ensure that new payments infrastructure is not developed without factoring money laundering, fraud and other concerns into their designs.

Finally, the paper has welcomed the UK government's intention to create a UK public-private economic crime data strategy and noted some key considerations the strategy might want to reflect. Most critically, the strategy must seek to maximise the data coverage offered by information-sharing utilities and create mechanisms for further data sources of importance to be onboarded as they emerge over time. Thought also needs to be given to how to leverage the power of private competition and innovation whilst making sure these forces remain aligned with overarching strategic goals. Similarly, the strategy should look to strike the balance between information-sharing effectiveness and data privacy, and the realisation of quick wins versus the longer-term construction of key information-sharing infrastructure.

Again, looking beyond the UK, other countries should appraise their information-sharing strategies or set the objective of creating one. The key strategic considerations will vary by geography: in many countries, the focus may be on initiating the first round of pilots; in others, like the UK, there may be more of a need to coherently frame the volume of activity that is already taking place.

However, to reiterate the key message of this paper to policymakers: information sharing can have a transformational impact in the fight against economic crime and national payments systems have significant potential in supporting and accelerating it. There are opportunities now to make better use of existing points of data aggregation and these should be taken. More widely, the introduction of ISO 20022 presents a once in a generation opportunity to transform information sharing in the fight against financial crime both domestically and globally. Ongoing reviews of payments transparency by both FATF and the G20 are welcomed but must promote the fight against financial crime as a key policy objective in that context. It is only through such reforms and innovations that we might begin to drive meaningful improvements in effectiveness in the fight against financial crime.

Contacts

Andrew Robinson

Partner and Strategic
Advisory Leader
andrewrobinson@deloitte.co.uk

Chris Bostock,

Director, Head of Deloitte's
Global Forum for Tackling
Illicit Finance
cbostock@deloitte.co.uk

Luisa Brana

Technical Director,
Financial Crime
lbrana@deloitte.co.uk

With special thanks to Will Tilston for his contribution to the development of this thought piece

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please click here to learn more about our global network of member firms.

Designed by CoRe Creative Services. RITM1509403