payments strategy forum

November 2017

Payments Transaction Data Sharing and Data Analytics – Strategic Solution – Scope and Governance Oversight

Contents

Background

Payments in the UK can be made using multiple payments mechanisms (e.g. Bacs, CHAPS and Faster Payments). These payments systems can be used by criminals to launder stolen or misappropriated money, masking the trail of funds and making its origin unclear. This laundered money can be used to fund terrorism or organised crime, or allow criminals to profit from fraud.

In the Payment Strategy Forum's (the Forum) strategy published in November 2016, 'A Payments Strategy for the 21st Century' (the Strategy), the Forum proposed a Payments Transaction Data Sharing and Data Analytics solution to help fight financial crime that occurs through the misuse of payments systems. The solution will enable visibility across different transactional data sources to create a rich data repository and analytical capability.

The objective of the solution is to detect and prevent current and future financial crime by creating an industry-wide capability to analyse end-to-end payment transaction data from all retail interbank payment mechanisms in conjunction with other relevant sources of diagnostic information. Examples of financial crime being targeted include: the identification of money mule accounts and the ability to return stolen money.

The Forum has recognised that whilst its focus is on strategic solutions, the current industry led and funded tactical solution should be seen as an opportunity to develop and test concepts that could form part of a strategic solution.

The tactical solution was initiated in early July with FPSL as a delivery body for implementation; this solution will transition into the NPSO at the end of 2017. The tactical solution will provide early benefit to aid the detection of money mule accounts, and pilot methods for funds repatriation. The tactical solution will run as an interim service, until the strategic solution is implemented.

In July 2017, the Forum consultation 'Blueprint for the future of UK payments' gave an initial proposal for the strategic solution. Following these responses, the Forum conducted further work and discussion to develop the solution. This document provides an overview of the scope and governance oversight for the proposed strategic solution, and is intended to provide details of the solution such that an appropriate solution delivery body can carry forwards the further analysis and development required to implement the solution. This document includes the additional information gained from responses to the Forum consultation, as well as the further work of the Forum's working group.

1 Overview of Strategic Solution

1.1 Objective of this Document

The 'Payments Transaction Data Sharing and Data Analytics" strategic solution is a culmination of a number of activities begun in December 2015 with the aim of handing over to the New Payments System Operator (NPSO) in December 2017. Figure 1 below illustrates the timeline.

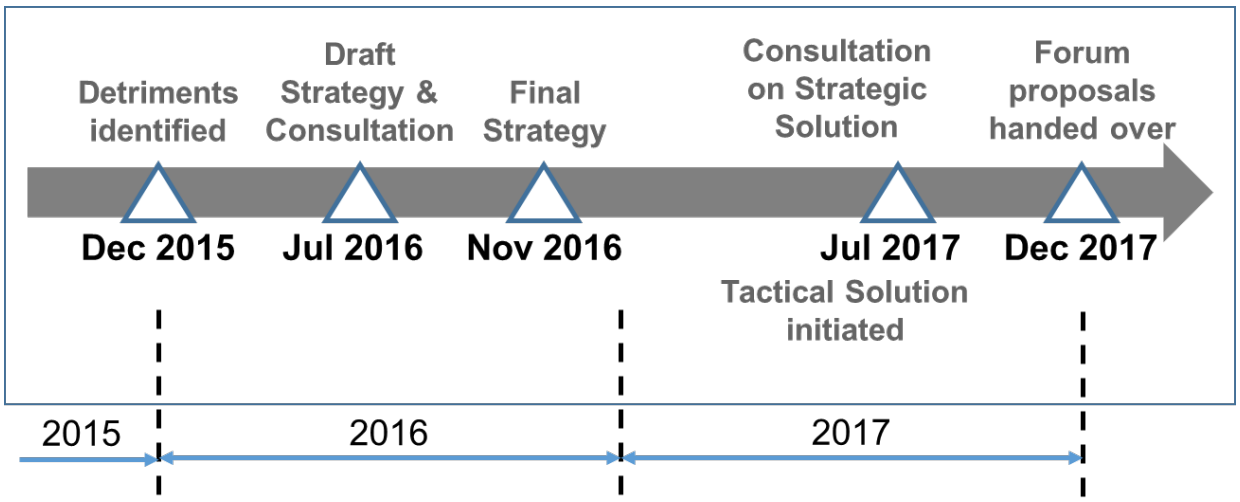

Figure 1 Financial Crime Working Group – Activities Timeline

This document defines the suggested scope of a payments transaction analytics and data sharing strategic solution, including a central set of standards that should be developed, and the ability to enrich payments in real-time, with the whole solution overseen by a governance body. The standards and solution design should be reviewed and validated with representatives from the financial services industry, service providers and other key stakeholder groups.

A companion document details the solution implementation approach to be taken.[1]

1.2 Strategic Solution Description

The strategic solution will consist of three core capabilities:

- Ability for participants to access payments transactions and other contextual data from a wide range of sources.
- Ability to securely store several years' worth of this data in accessible form to a certain set of trusted participants in order to enable historical payments fraud analysis.
- Ability for properly governed participants to deliver advanced data analytics on the payments transactions and other data that is acquired in order to identify and prevent payments fraud.

[1] "Payments Transaction Data Sharing and Data Analytics – Strategic Solution - Solution Implementation.pdf"

The solution must meet these key requirements:

- Provide timely secure access to both detective and preventative analytical tools and information that enable measures to be taken by Payment Service Providers (PSPs), the New Payments System Operator (NPSO), public bodies (i.e. central and local government), and law enforcement agencies to address identified incidents or trends.
- Be adaptable to new types of payment mechanisms.
- Be adaptable to new financial crime threats.
- Include all PSPs and all payment types to ensure sufficient coverage is available to enable analysis of full payment journeys.
- Support a competitive market for the supply of tools, analytical insight and other relevant services for each of the core components.
- Have appropriate linkage to the New Payments Architecture (NPA) for the acquisition of payments transaction data.
- Provide significant additional detective and preventative capability compared to the tactical solution and be scalable in terms of volumes, types of transactions and financial crime threats.

Figure 2 (below) provides a conceptual view of the proposed strategic solution which will provide the capability for end-to-end analysis of payments transactional data, spanning the whole payments community.

Points to note:

- Participants in the solution will include financial institutions that offer financial accounts to customers (e.g. a bank or insurance company), as well as a mixture of other participant types that will be looking to provide analytical insight on payments data or otherwise disrupt financial crime and promote customer security.
- The strategic solution will define a set of standards and quality requirements for messaging APIs building on the open banking API definitions. This messaging will enable authorised participants to share payments data, contextual data, and derived intelligence, thus allowing participants to conduct data analytics activities on the full payments transactions data set available.
- Strong controls and governance will be put in place to ensure security and privacy of transaction data whilst enabling effective financial crime analysis. Existing and known future regulatory requirements will be accounted for, acknowledging areas where regulatory change may be required to help address financial crime (e.g. for the purposes of funds repatriation).
- The solution design will be built into the NPA to give the capability to have access to NPA data, as well as perform real time enrichment of data as an NPA payments message is processed.

It is proposed that Application Programming Interface (API) technology is used as one of the technologies to connect the components together by utilising a common data and communications standard, building on the work already undertaken by Open Banking and the PSF New Payments Architecture (NPA).

A part of the solution design will include real time information provision, transaction analysis and alert generation, in order to prevent fraudulent payment flows. The sharing of data will allow for more in depth trend analysis that will be driven by monitoring historical transactions across a wider range of payment types/data. This will in turn derive insights and patterns that can be fed into the real time analytics and financial crime information systems.

1.3 Strategic Solution Conceptual Design

It is proposed that the strategic solution design will enable:

- Industry wide data sharing covering payments and other relevant contextual data
- Industry wide intelligence sharing, allowing the tracing of payments between different payments mechanisms
- The ability to perform interaction with NPA payments and other payments schemes in real time

The conceptual design of the solution can be seen in Figure 2 below.

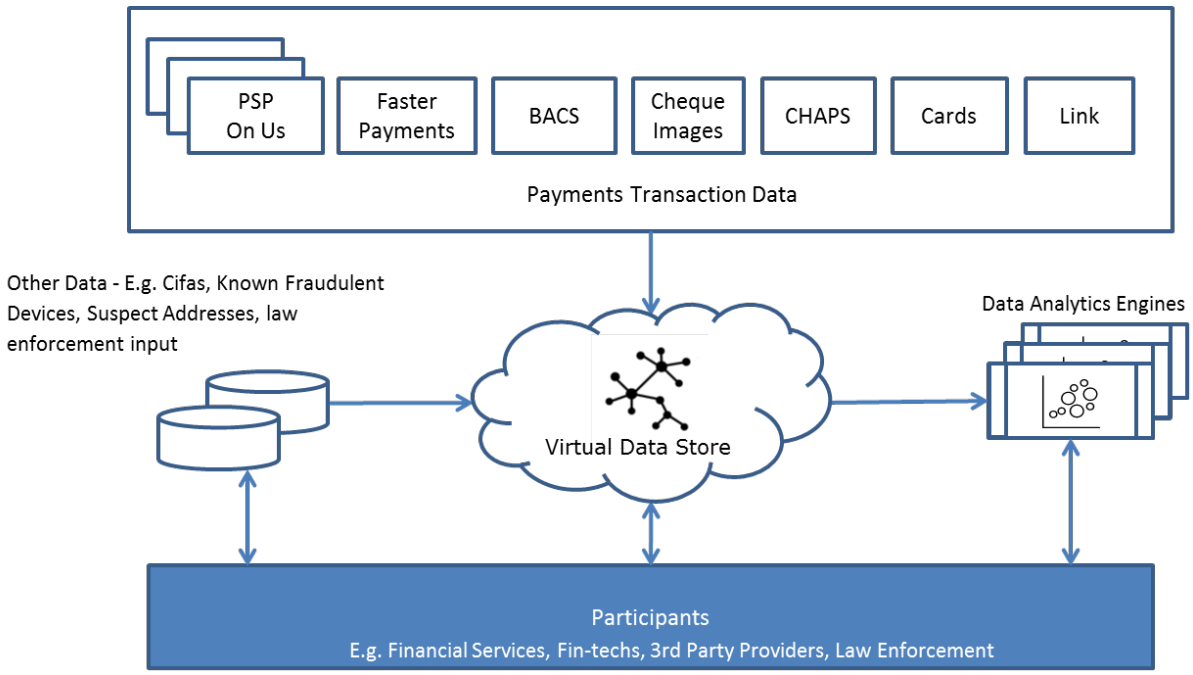

Figure 2 Conceptual view of transaction data analytics strategic solution

The design has several key elements:

1. The creation of a virtual data store by combining API messaging.
2. The creation of a capability to provide access to query the sources of data, as well as receive or distribute intelligence which can then be shared with other participants.
    - This will also allow for real time interaction with NPA payments (and other payment schemes) whilst the payments are in-flight.
3. The ability to receive payments transaction data from a wide variety of sources.
4. The ability to receive contextual data from a wide variety of sources.
5. The ability to enable data analytics to be performed via multiple engines from multiple providers.
6. The ability to allow interaction between multiple types of participants to different sources of payments transaction information.

The intent of the solution is to establish an environment in which information can be shared, received, and actioned effectively between participants in different areas of the payments community. This interaction is currently limited within the industry, which is preventing the ability to trace payments fully end-to-end. Without being able to trace these payments fully, detection and prevention of financial crime is hindered.

The design is intended to establish this data sharing capability whilst also promoting competition and targeting innovation within the market with regard to the provision of analytics services. By allowing better access to all the required data, this will allow insight providers to innovate quickly to detect and prevent newly identified and emerging financial crime trends. This competition and cross industry data sharing capability is not linked to any payments mechanism, and thus once established, participants within the industry (or the industry as a whole)

can begin to detect and prevent financial crime that would previously have remained undetected, by allowing access to the end-to-end payment journey.

A key feature of the design, separate to the ability to share data and insight, is the ability to perform real time intervention of in-flight payment. The scope of the design is initially linked to the NPA payment mechanisms, but could in time expand to include other payment mechanisms. Analytics performed across the full payments journey can be used to inform real time payments monitoring systems that can evaluate any risk indicators for payments in real time. The intent is that all payment mechanisms will be able to connect in order to disrupt criminal behaviour and more effectively return funds to victims.

The solution implementation has been split into two parallel strands of activity each with their own associated timeline. Strand 1 will look to establish the data sharing environment, so that cross industry end-to-end payments analytics can be enabled in the shortest possible time. Strand 2 will look to establish the ability of the NPA to connect to the strategic solution along with the development of the NPA to eventually allow real time payment monitoring and financial crime disruption.

1.4 Solution Minimum Scope

The strategic solution will be designed to enable coverage of all transactions made by any payment mechanism, to or from every customer account domiciled in the UK, covering a defined minimum time period. The participants of the strategic solution will provide access to stored payments transactional data, or other contextual data, to allow for analytical tools (central or otherwise) to be performed over that data. The insight gained from this analysis would be shared with other participants, to help prevent financial crime.

Based on current payment mechanisms and storage / analytical technology, a minimum scope for initial implementation of the strategic solution in the timeframe detailed in the implementation plan is as defined below:

- Payments above a minimum value threshold based on transaction type, with the ability to reduce or remove this threshold over time.
- Payments made using the core UK domestic electronic schemes, card payments, international payments, internal bank payments and transactions (including future derivations of these payment types).
- At a minimum, payments made to or from personal current accounts and business current accounts, with an ability to add additional account types as required.
- Diagnostic and contextual information (e.g. known fraud and other financial crime related information) based on availability and relevance.

Where data that exceeds these requirements is available, this will be included if practical. It is expected that the solution capability will expand beyond this minimum scope over time.

Whilst the objective is to cover as many payments systems as possible, it is recognised that some sources of data may not form part of the initial solution based on the complexity and costs of inclusion. Any transactional source that is not part of the initial solution runs the danger of financial crime migration (i.e. criminals may start to use those payment mechanisms to move money). These transaction sources may be subsequently used to hide the trail of funds, or allow laundered money to enter the UK payments market.

The solution must be capable of processing all of the information held to either identify threats and trends, or to specifically look for transactions associated with a particular type or instance of financial crime. The solution should:

- Be able to run at all times and provide results immediately on demand.
- Be capable of handling a wide range of criminal activity, ranging from third party payment fraud, beneficiary fraud and application fraud through to benefits fraud or terrorist financing.
- Be capable of predicting criminal activity based on patterns of behaviour, enable risk-based scenario modelling, as well as identifying impacted customers (such as fraud or scam victims).

- Provide and support mechanisms to allow continuous feedback to participant organisations to help better understand financial crime activity, and so inform development of participants' internal policies and processes to counter financial crime.

Table 1 below shows the likely participants in the strategic solution.

Category	Participant
Information Providers & Consumers	PSPs
	Payment Schemes
	Card industry participants
	Government
	Law Enforcement
	Fraud Investigators
	Financial crime prevention agencies (e.g. Cifas)
	3rd party PSPs
	Regulated Third Party Service Providers (TPSPs)
	Money transfer services
	Crypto currency services
	PSPs internal fraud prevention teams
Information Providers	Cifas
	Credit Bureaux
	National Hunter
	FISS
	Credit reference agencies
	Reference and other data providers – metadata provision
Service / Solution Providers	Data storage
	Data Analytics Service Providers
	Cloud Service Providers
	Financial crime prevention security solution vendors

Table 1 – Strategic Solution Participants

The solution governing body should not place restrictions on participants within these categories, other than to safeguard against illegal or inappropriate use or ensure the safety and security of the data. Other valid participant groups may emerge over time. Therefore, the solution should not be limited to the original categories of participants and should be scalable and flexible to support future categories that may emerge such as those relating to distributed ledger technology and virtual currencies.

1.5 Links to other systems and financial crime initiatives

The development of the solution must consider the necessary interactions and links with other systems, transactional data sources and financial crime initiatives such as those available from government agencies, HM Treasury, and reference data agencies.

In particular, the appropriate linkage between the solution and the implementation of the NPA must be considered, and appropriate design decisions made to reflect this. This includes real-time capabilities within the clearing layer of the NPA architecture.

Linkage to the NPA

The NPA architecture must be designed in such a way as to support the enrichment of data as it is passed between participants.

As the NPA transports attended messages from sending banks, it must pass data to financial crime systems in real-time for data enrichment and pass this enriched message on to the receiving bank.

The NPA should provision the payment messages received to financial crime systems as and when received. In particular, for unattended payments of bulk transactions, this process should occur in line with the NPA time horizons.

The NPA will make available the entire payment message processed to the financial crime system. This would include all types of payments with any defined enhanced data fields included.

Linkage to other data sources

The solution should, over time, also link or align to other Forum financial crime initiatives and solutions (including Financial Crime Data and Information Sharing, Trusted KYC Data Sharing, Guidelines for Identity Verification and Authentication and Risk Assessment).

The solution should link to other relevant industry sources of data that can provide additional contextual information to help detect suspicious payments activity.

Combining information from these different sources has the potential to provide huge benefits for the detection and prevention of financial crime, as well as improving process efficiencies for PSPs and consumers.

Interdependence

Whilst the links between the strategic solution and other systems should be carefully considered, the implementation of the solution should not be reliant on the implementation of other payments industry initiatives, including the NPA. However, it is acknowledged that real-time interventions of NPA payment messages may only be possible through NPA implementation.

1.6 Split of Solution into Stranded Delivery

The strategic solution implementation will be split into two parallel strands of activity. The intent is to ensure the establishment of an effective analytics data sharing environment, which could provide cross industry benefits in the short term and is not dependent on the implementation of the NPA.

Strand 1 - Standards definition to enable data sharing:

- Approaching analytic vendors and data provider organisations for input into the API solution.
- Defining the API technical standards.
- Defining data quality and data standards to provide full coverage of payment journeys for financial crime analysis.
- Defining and implementing methods and controls by which analytics vendors can access payments data for fraud prevention.
- Ongoing exploration of legal considerations for solution implementation, either regarding the sharing of information or the ability to effectively take action from the derived insight.

Strand 2 - Incorporate solution into NPA design for FPS, Bacs, ICS data:

- Ensuring that the solution is built into the work of the NPA.
- Embedding data quality requirements into the NPA designs so that the NPA captures the most suitable data to fight financial crime.
- Re-procuring the tactical solution to integrate to Strand 1 standards and work with the NPA.
- Once the NPA implementation is live, real-time interaction with NPA payments will be possible via the data sharing standards established by Strand 1.

Sections 3 and 4 of this document provide more details into the scope of each of these two strands.

1.7 System Use Cases

The solution should support both on-demand interaction, where participants can get feedback from the system in real-time, as well as longer running processes to develop deep analytical insight over large volumes of data.

On-demand interactions would involve participating organisations exchanging information with the solution in real-time. This could involve matching account information against known watch lists prior to authorising a transaction, or more general transaction risk scoring.

Longer running batch processes will run over large sets of data with the ability to use advanced analytical techniques (machine learning, artificial intelligence etc.), to support intelligence building. Potential benefits include recognition of new financial crime trends by observing unusual patterns of behaviour, or the identification of potential fraud and scam victims where the pattern of financial crime behaviour is known.

The strategic solution will allow the ability to combat a range of financial crime methods over and above the tactical solution (money mule account identification and funds repatriation for Faster Payments and Bacs transactions only), potentially spanning both private and public sector uses.

Some example use cases are outlined below. Whilst some solutions exist on the market that attempt to address these use cases, this collaborative solution would be uniquely placed to provide a comprehensive industry wide analysis with a full range of payments data. This would greatly enhance the value of such solutions, providing benefit for consumers, businesses and financial institutions as financial crime is detected and prevented with greater accuracy, efficiency, and speed.

Transaction Verification Services

Verification of payee identity and identification of abnormal account activity are just two examples of a large number of transaction verification problems faced by the payments community. The strategic solution could be used to address these problems at an industry scale, and is closely aligned to the ‘Assurance Data’ NPA solution that tackles ‘Confirmation of Payee’ use cases. For example, analysis of the core transaction data could provide account name verification, allowing the system to verify that a payment is going to the intended recipient (which would contribute to addressing Authorised Push Payment (APP) scams), thus reducing the chance of misdirection of payments and protecting against financial crime scam activities. The solution could also be used to combat a large variety of other transaction verification problems (e.g. identifying unauthorised transactions).

Fraud Victim Identification

Given a known pattern of fraud or scam activity, spanning multiple payments channels, analytical techniques could be used to identify potential consumer victims. Furthermore, at-risk customers could be identified and pre-warned of emerging financial crime threats prior to them being targeted or falling victim to crime. Combining different data sources in this way will enable proactive financial crime prevention. See Appendix A for further information on APP fraud.

Suspicious Activity Report (SAR) Investigation

The National Crime Agency (NCA) may be able to use the system to identify and investigate SARs. This capability may reduce the burden and cost on individual organisations for SAR reporting, improving efficiency and reducing cost within the industry.

Access to a single, comprehensive view of high quality payments transaction data may allow for increased accuracy, identifying criminal activity that may otherwise have remained undetected when data is split between different systems.

Funds Repatriation

In the case that law enforcement has taken action against owners of accounts used for fraudulent activity, the strategic solution could be used to repatriate stolen funds by tracing the original crime victim. The enrichment of payment messages with additional data will enable this identification and notification to PSPs across the network. See Appendix A for an example of funds repatriation.

Out of scope use cases

The Transaction Analytics strategic solution is not to be used for any form of non-security or non-financial crime purposes.

Safeguards must be put in place to actively monitor usage of the strategic solution in order to identify and take action against any inappropriate usage of the system.

The emergence and development of use cases

It is envisioned that potential use cases will develop through innovation within the competitive market for the provision of analytical tools and services. As part of solution development, participants should carefully consider where there may be benefit in establishing centralised shared analytics capabilities, versus where individual participant solutions are appropriate.

Any centrally developed use cases should be supported by appropriate messaging standards, operational models, business case and funding models. Use cases will likely emerge over time as innovation and demand emerges.

1.8 Enabling Competition

The strategic solution system architecture must be designed to encourage competition between analytics solution providers.

By allowing standardised access, analytics service providers will be able to compete to add most value to PSPs and other system participants.

A core set of data exchange services will be provided as part of the solution whilst standardised access to system participants and payments data will be enabled for analytical services to provide analytical insight.

Further work is required in order to define the full set of standardised services to be provisioned as part of the solution and this definition should be included in the scope of Strand 1.

1.9 Data Security and Access

All work done in solution design should take into account the dramatic transformation currently underway within the payments community, driven by the EU and UK government initiatives.

A privacy impact assessment and clear guidance from the Information Commissioner's Office (ICO) must be sought in order to ensure that all appropriate legal considerations are identified.

The impact assessment will enable strong controls and governance to be put in place to ensure security and privacy of transaction data whilst enabling effective financial crime analysis. As a minimum, existing and known future legal and regulatory requirements, topics and guidance are recommended to be taken into account when defining the transaction data sharing and data analytics standards (see Figure 3).

Examples of Regulations, topics and guidance with impact on transaction data sharing and data analytics standards

- 4th Money Laundering Directive (MLD4)
- Payment Services Directive 2 (PSD2)
- EBA PSD2 SCA Regulatory Technical Standards (EBA RTS)
- Joint Money Laundering Steering Group Guidance (JMLSG)
- UK HM Government guidance (GOV.UK)
- FCA Financial Crime Guide (FCAFCG)
- European Electronic Trust Services Regulation (eIDAS)
- EU Funds Transfer Regulations (WTR2)
- UK Data Protection Act (DPA)
- EU General Data Protection Regulations (GDPR)
- UK Money Laundering Regulations 2017 (MLR)
- UK Payments Accounts Regulations 2015 (PAR)
- EU Payments Accounts Directive 2014 (PAD)
- UK Current Account Switching Service (CASS)
- CMA 'Retail banking market investigation' report

Figure 3 Regulations and guidance with impact on transaction data sharing and data analytics standards

2 Governance Body Oversight

One of the first steps towards solution delivery will be to establish a governance body that will oversee solution development and provide ongoing oversight of the strategic solution environment. The governance body should be formed to represent the views and interests of a wide variety of stakeholder groups.

Overall responsibilities of the governance body will include the following activities:

- Define the standards regarding the sharing of data by participants.
- Evolve the standards to meet the needs of the whole range of participants.
- Enforce compliance to the defined data analytics standards.
- Encourage usage by all participants in the payments environment.
- Establish a process for authentication and policing of third party analysis providers.

Once a data analytics provider has identified a valid fraudulent pattern as a result of their data analysis, they will be mandated to feed these results back into the central community.

The governance body should determine the correct methods and processes for this feedback function as well as determine proper ownership and responsibility for managing this process.

2.1 Evolution of the Data Sharing Standards

The continued evolution of the standards will be key to ensure coverage of future regulatory requirements and adoption of the solution by all participants. It will also maintain an open data analytics environment with no barriers against smaller participants joining. The amendment of existing standards and/or the inclusion of new standards by the governance body will ensure the environment evolves on an ongoing basis to cover the needs of the whole range of participants.

A large number of analytics service provides must be able to co-exist together in the open data analytics environment. It is key that this environment does not impose any restriction that may limit the competition in the market.

The governance body, will go through an appropriate consultation process on a yearly basis, engaging with participants to ensure that the data analytics standards are appropriate, accepted and understood.

2.2 Compliance and Correct Interpretation

The different participants in the data analytics environment may interpret the standards in different ways. Therefore the data analytics standards must be written clearly and with a high level of detail. The governance body must oversee that the standards are understood and respected by all the PSPs and service providers by providing a validation process and methodology for data analytics models and methods. An authentication service would include back testing and auditing functions to prove the value of data analytics results.

For the correct interpretation and accurate understanding of the standards, educational sessions should be provided to the different range of stakeholders. The governance body must define the strategy and methodology for the provision of these sessions. Sessions should be held before the solution goes live and when a significant change is made to any of the existing standards.

Continuous feedback will enable the governance body to answer questions raised by the participants and make further enhancements.

Compliance and complaints management

The governance body will have to determine and formally document official procedures to cover non-compliance with the data sharing standards or for the usage of the solution for inappropriate means. The governance body will also have a responsibility to receive, address and respond to any complaints made against solution participants.

2.3 Management Information

A number of metrics must be monitored by the governance body on a periodic basis through service providers to track as a minimum:

- Level of adoption of the data analytics initiative.
- Any key issues reported by the different participants.

These metrics will be key to ensuring that the environment is meeting participant expectations and is achieving the right level of adoption across the industry.

3 Strand 1 – Standards Definition and Data Sharing

Implementation of the solution will be split into two parallel strands of activity. Figure 4 shows the split of Strand 1 and Strand 2 solution coverage with Strand 1 covering the API standards and the enablement for analytics providers, PSP’s and other payment schemes to communicate with each other in a controlled and standardised method. Strand 2 includes the ability of the NPA to connect to the strategic solution as well as the real-time enrichment capability as part of the NPA development.

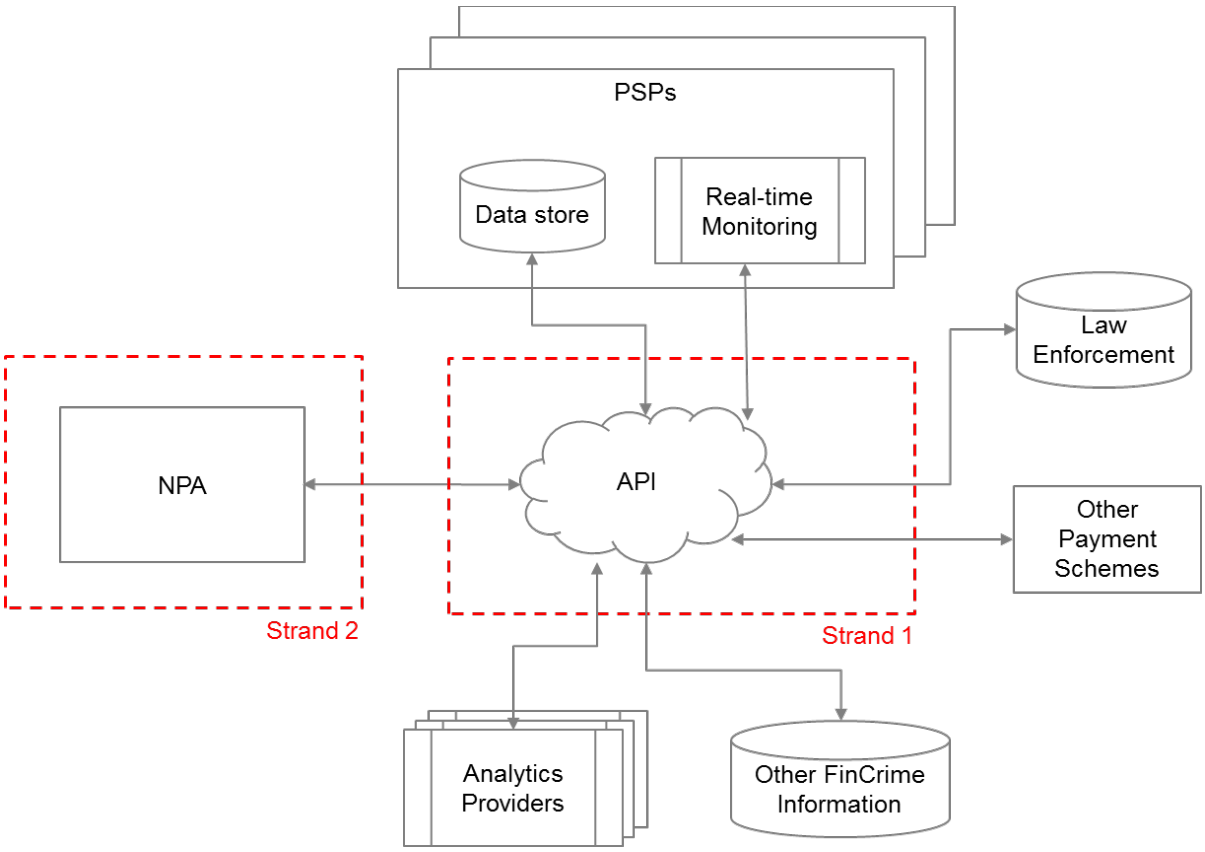

Figure 4 Strand 1 and Strand 2 scope coverage

Strand 1 scope is focussed on establishing the standards for participant communication across the system for sharing of transaction data and analytics analysis information. It covers all existing payments schemes and systems including but not limited to:

- PSP on us
- Faster Payments
- BACS
- Cheque Images
- CHAPS
- CARDS
- LINK
- Electronic Wallets (i.e. PayPal)

3.1 API Solution Use Case Validation

The definition of the API based solution, API standards and data standards will require consultation with relevant stakeholders including analytics vendors and data provider organisations as well as the NPA design authority.

The Governing Body should organise consultation sessions with stakeholders to gather input and validate cross-participant use case definitions.

The strategic solution will enable communications between multiple payment systems participants and therefore validation should be sought for use cases that utilise the unique nature of the strategic solution.

3.2 API Technical Standards

Open Banking API definitions should be used as the starting point for the Strategic Solution API standards which should be designed to be extensible for future proofing of additional message types, operations and capabilities.

All aspects of the API technical standards including message types, Data enrichment types and control mechanisms will need to be defined and maintained by the Governing Body.

3.3 Data Quality and Data Standards

The data quality and data standards will need to provide full coverage of payment journeys for financial crime analysis. Therefore the design of these requirements must take into consideration the full end to end payments flow including accounting for data entering or exiting the solution from non-UK based systems.

3.4 Defining Methods and Controls for Data Analysis

The participants to the solution will provide access to payments transactions originated and received by them using the API technical standards across their systems. Data analytics participants and other participants will be able to make requests for payment transaction data using these APIs.

There may be a requirement for standardised services to enable effective participant communication.

The Governing Body will define and maintain the methods and controls by which this access will be provided.

3.5 Assessment of required legal framework and legislative change

The implementation of the solution or solution use cases may require legislative change or other key legal considerations. The governance body will work with appropriate industry experts or other organisations to identify and overcome these legal barriers, either to the exchange of information, or for the utilisation of derived insight.

4 Strand 2 – Service Procurement and real-time NPA payment interaction

Implementation of Strand 2 will provide the ability to send messages to or receive messages from solution participants that will be the primary means of interacting with NPA payments in real-time.

Figure 5 below illustrates the messaging flow by which an NPA payments transaction message can be enriched in real-time. By utilising the standard API's defined in Strand 1 and the connectivity provided by the Strand 1 architecture it will be possible to enrich payment transaction messages with analytic data provided by 3rd party data analytics services.

A payments transaction passing through the Clearing & Settlement layer of the NPA will make an API call to a 3rd party data analytics service and will provide the results back to the NPA Clearing & Settlement layer.

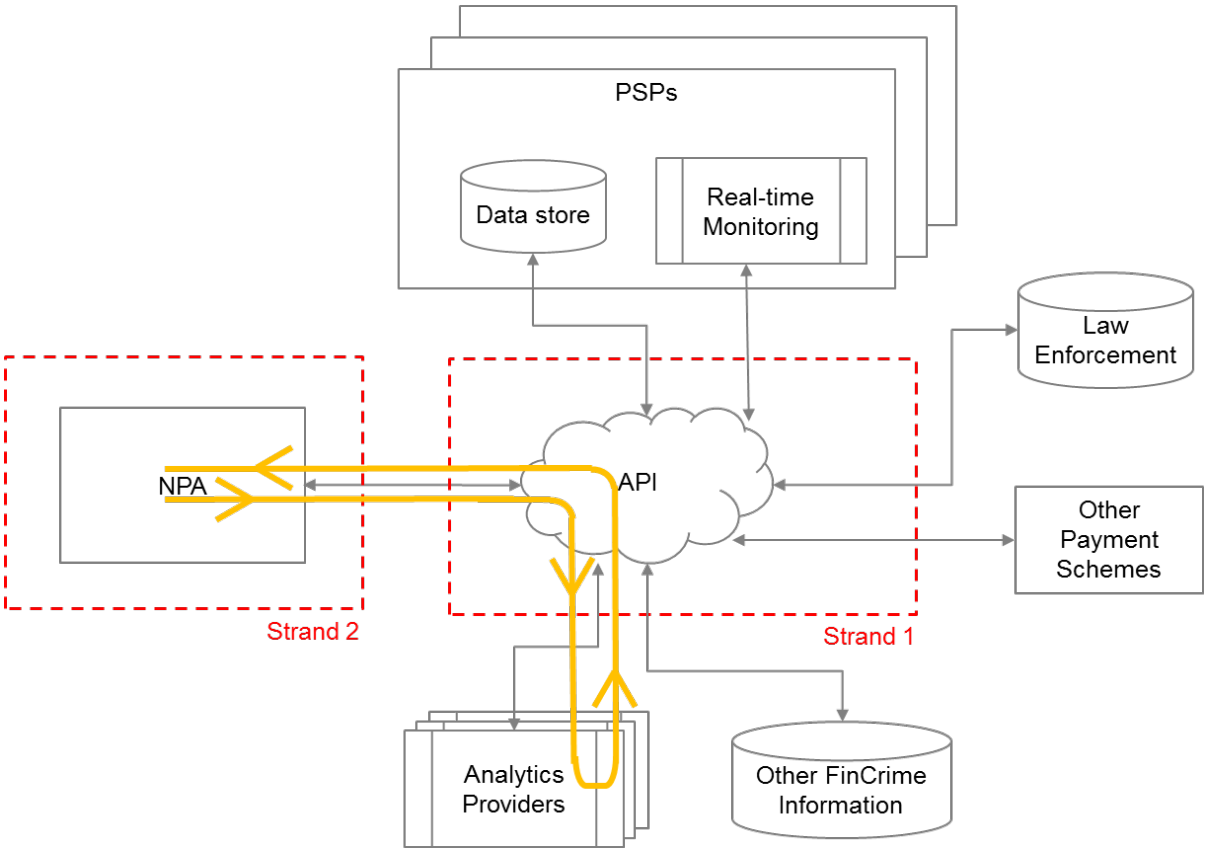

Figure 5 Usage of Strand 2 for real-time data enrichment

4.1 Building into the Work of the NPA

The Transaction Analytics Strategic Solution Governing Body must work with the wider NPA management and implementation teams to ensure that the Strand 1 capabilities and requirements are included in the NPA designs.

Any re-procurement of current scheme systems and infrastructure by the NPA must include the requirement to conform to the strategic solution Strand 1 standards and capabilities definitions.

The aim being for the NPA mechanisms to be fully integrated into the wider payments transaction analytics solution at go live.

4.2 Include Data Quality Designs in the NPA

As the NPA re-procures existing systems, the data quality standards defined in Strand 1 must be used and built on to support the specifics of each system and the payments transaction analytics requirements.

Each NPA system will have specific data requirements and data provisions which can be leveraged to provide analytics capabilities for specific financial crime use cases.

4.3 Re-Procuring the Tactical Solution

The scope of Strand 2 also includes the re-procurement of the Transaction Analytics Tactical solution so that the replacement system includes the expanded scope of the strand 1 capabilities and requirements and works to provide central analytical capabilities to the NPA payments mechanisms.

The strategic solution Governing Body will need to work closely with the NPA to ensure that the re-procurement activities integrate the transaction analytics capabilities without a loss of function.

4.4 NPA Integration to Strand 1 Capabilities

Part of the agreed implementation plan of the NPA and its components must include integration and user testing of the data analytics capabilities that have been established as part of the strand 1 activity.

A real-time data enrichment capability must be included in the scope of the NPA so that transactional and other forms of messages flowing though the NPA can be enriched with financial crime relevant data from participants of the transaction analytics strategic solution.

Use cases must be determined for solving financial crime detriments with the use of alerting and notification functionality enabled by the enriching of transaction messages as they pass through the NPA.

The participant data access requirements defined as part of Strand 1 must also apply to the NPA systems.

The strategic solution Governing Body will need to work closely with the NPA as part of this planning to ensure that there is continuity of service and no adverse impacts on current or future participants.

5 Applicability of Data Analytics Standards

The strategic solution will create a standardised approach to sharing data analytics information that participants should adhere to. These standards will focus on defining the characteristics of the data analytics i.e. data fields that will be shared and the technical standards of the data analytics technologies.

The initial implementation of the standards is recommended to cover only the sharing of a core set of transaction data between participants and data analytics service providers depending on chosen data analytics scenarios. The initial scope of the standards will be defined through an initial design development and proving exercise (see implementation approach document for further details) to understand what types of message will need to be sent for the sharing of:

- Payments data
- Contextual data (e.g. customer account information, KYC information, known fraud cases etc.)
- Derived intelligence (e.g. an account that has been identified that received stolen money, but where the money has not or cannot be tracked any further).

Message types and usage scenarios will need to be agreed following the design development and proving exercise. Examples of useful scenarios to consider could include:

- APP Fraud (See Appendix A for use case example description)
- Money mule account fraud
- Phone scams

The scope of the standards will evolve incrementally as the solution offerings expand and new regulatory requirements emerge (e.g. extensions to the data model and additional security requirements). The baseline standards should cover the following topics (see Table 2).

Topic	Content
Sharing capabilities and interoperability (see section 6)	Defining the data sharing mechanisms between participants, e.g. consent process and cooperation recommendations to ensure that both sender and receiver of payments data contribute.
Data model (see section 7)	Defining the data model including completeness requirements and data access rights. A minimum set of fields will be defined that ensures flexibility for different payments processes and regulatory requirements.
Security and privacy (see section 8)	Providing technical details for security and encryption by cross referencing to Open Banking, PSD2, GDPR and ISO. Also defining reporting requirements for participants if they experience security and data breaches.
Governance body oversight (see section 2)	Activities include evolving and enforcing the defined payments messaging standards as well as identifying which service providers are not compliant with these standards and taking appropriate actions.

Table 2 Data sharing standards topics

These topics will each cover, where necessary, the behavioural requirements of participants, the technical requirements to be met by participants, and the oversight required by the governance body.

These topics may have been addressed already for the purposes of Open Banking and PSD2. The governance body will need to draw on the progress made in each of these areas. Other standards related to sharing data are available (such as OAuth 2.0 and the Open ID Connect protocols), but are not specifically designed for use in association with analytics services. The proposed analytics data standards will be complementary to these and it is anticipated that all standards will develop over time to meet the needs of the evolving market place.

6 Sharing Capabilities and Interoperability

The technical standards defined as part of Strand 1 must cover the sharing capabilities of multiple participants, including those that want to share or receive payments data, those that want to share or receive additional data for use in analytics, or those that want to share financial crime insight; the sharing of this data is to facilitate the provision of financial crime detection and prevention analytics services.

In most cases, the participants will act both as providers of and receivers of data. This solution will only have maximum benefit if solution participants are willing to share not only their payments and contextual data, but also the results of their analysis with the other solution participants (e.g. identified high risk accounts or transactional patterns). For example, data analysis could identify criminal networks and compromised bank accounts. Once identified, there should be a requirement for participants to notify relevant parties so that action can be taken and future analysis can be improved.

6.1 Data Sharing Principles

Participants should establish data sharing behaviours that allow connectivity with other participants, allowing participants to request and receive information from other participants.

Participants should be willing to share, at a minimum, the data as defined in the associated data model standards. Participants should be able to share additional information exceeding the defined minimum set if relevant and as analytic requirements evolve and new use cases are defined.

PSPs and data analytics service providers will be able to register their participation in the data analytics environment. This registration will contain information about the services supported by the participant.

6.2 Degree of Oversight Required

The governance body must ensure that the standards evolve on an ongoing basis to cover the needs of the whole range of participants. In addition, the governance body will supervise the participant authentication process in order to ensure compliance with the data sharing standards. Participant authentication may be revoked if participants are no longer meeting the required standards.

The governance body should continuously monitor the conduct of solution participants to ensure compliance with standards and the usage of data for appropriate purposes.

7 Data Model

It is recommended that the governance body define a data model associated with messaging standards including a minimum set of data fields and the data exchange format (e.g. ISO20022).

7.1 Data Model Requirements

Authorised participants must ensure that the data fields exchanged are aligned with the agreed data model; covering completeness (e.g. provision of the right amount of information) and formatting (e.g. provision of the datetime data field in the right format such as: "yyyy'-'MM'-'dd'T'HH':'mm':'ss"). To protect their customers, participants (financial institutions in particular) will have to establish and maintain controls on the personal customer information that they are holding and/or providing to others.

The data model must enable a variety of message types to allow data sharing between participants. This is likely to include, as a minimum, the ability to share payments data, supplementary contextual data (e.g. device information, account address, or KYC data to be used for analytical purposes), and derived insight data (to share insight from analysis of the data). It should also be flexible to provide for future use cases and as yet unknown analytical techniques and processes. It will likely be made up of a number of different message types including payments, notifications, requests and alerts.

7.2 Degree of Oversight Required

The data model will need to be strictly controlled to ensure that legal and regulatory requirements are being met and that the system is not being used for any non-financial crime purposes.

8 Security and Privacy

The standards must define security and privacy rules for information shared between solution participants to protect the system participants from fraudulent actors.

8.1 Security and Privacy principles

With the objective of maintaining an environment in which sensitive customer data remains safe, participants will be required to report any kind of confirmed or suspected data or security breach in line with existing and known future regulations. Participants will be notified in the event that their data may have been compromised. Participants will be required to encrypt information shared with other participants. This will be key to ensure the security and privacy of data transmissions within the environment.

To protect payments and analytics data from access by 'bad actors', participants within the environment will be authenticated to guarantee that their processes are compliant with the defined security and privacy standards. The standards will be aligned with and cross-referenced to other regulations/initiatives like GDPR, Open Banking and PSD2.

All data analytics engines within the environment must provide participants with control over their data.

8.2 Degree of Oversight Required

All potential participants must be first accredited by the governance body to ensure compliance with privacy and security requirements. On an ongoing basis, the governance body will:

- Decide on required updates to the security and data standards to comply with regulatory change, mitigate emerging financial crime trends and to incorporate feedback gained from participants through usage of data and security protocols.
- Assess data analytics service offerings provided by the service providers to grant, review, revoke, or reinstate authentication to the participants within the environment.

9 Solution Commercial Model

9.1 Funding Approach

Once established, the Governance Body must work with industry stakeholders to define a funding approach for each of the solution strands. It is suggested that key principles are developed with the following as illustrative examples:

- The Transaction Data Sharing and Data Analytics solution is to be run as a not-for-profit service to the payments industry.
- Distinction should be made between the funding requirements for initial development and investment, versus the ongoing cost of running the service and maintenance.
- Basic usage of the Transaction Data Sharing and Data Analytics solution is based on participants paying a fee to use the information outputs of the service, potentially offset by the level of information input to the system.
- Only participants deemed authorised by the Governing Body are able to access or benefit from usage of payment transactional data available through the solution.
- The calculation method for participant fees should be subject to consultation so as to ensure an optimal model is identified which incentivises usage by as wide a range of participants as possible.
- Careful consideration should be given to a pay-per-use model for volume and usage based pricing as an addition to or substitute for the participant fees.

9.2 Solution Participant Funding Contribution

Different types of participants are expected to use the solution in different ways. This will need consideration and categorisation by the Governance Body, but as an illustration could include:

- PSPs who will have the ability to use the system to reduce their risks and exposure to the costs of financial crime.
- Law enforcement agencies who will have the ability to use the system to identify criminals and reduce instances of fraud.
- Data analytics providers who will be able to use the system to access transactional and historical payments data in order to offer analytical results and services to other solution participants. They are likely to charge a fee for these services to other solution participants.
- Many other uses of the solution will be possible which will provide benefits to different stakeholders.

The Governing Body should establish pricing models with a range of fees to be paid by each participant based on the method and type of usage of that participant.

Appendix

Appendix A

Use Case Example - Authorised Push Payment (APP) Fraud

A transaction analytics solution, enabled by the defined strategic solution, could be particularly beneficial when detecting and preventing APP scams. It is important to note that the strategic solution is intended to reduce a wide range of financial crime threats, not just APP fraud, and that the solution design itself does not contain specific requirements to target certain types of financial crime threat – these will develop over time as the solution design is further developed, and as the competitive market innovates to tackle new scenarios. It should also be noted that there are other PSF Improving Trust in Payments Solutions that will be of benefit in reducing the scale and impact of APP fraud, such as Consumer Education and Awareness, Financial Crime Data and Information Sharing, Guidelines for Identity Verification, Authentication and Risk Assessment, and Trusted KYC Data Sharing.

The Role of Payment Transaction Analytics

A characteristic of APP fraud is that the payee is a ‘real’ account holder (i.e. not a hijacked or impersonated account) and that the victim is convinced that the payment is legitimate and therefore insists on the payment being made, often when explicit advice is given that the payment could potentially be to a fraudster.

In this instance the PSPs involved in processing the transaction require specific knowledge of fraudulent activity before they can legally prevent the payment being made. In the absence of specific financial crime information associated with a payee account holder, transaction analytics can deduce that fraudulent activity is taking place by detecting patterns of related payments that are highly likely to be associated with hiding the true ultimate beneficiary.

An example of an APP fraud that exhibits such a pattern is shown in figure 6 below.

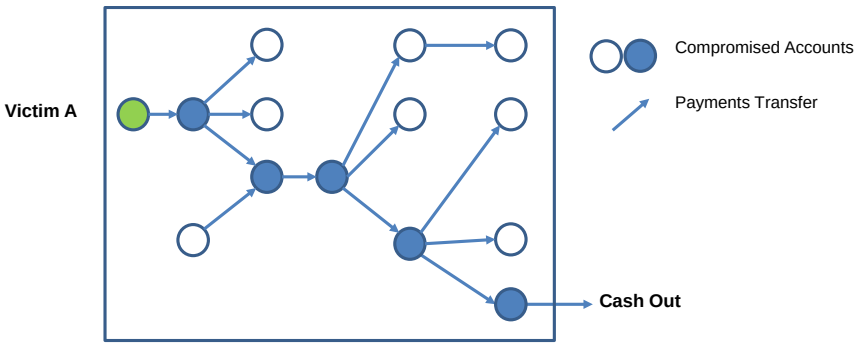

Figure 6 – APP fraud pattern example

Money is transferred fraudulently from "Victim A" to an account controlled by a criminal. This could be 'authorised' (APP Fraud) or any other type of 3rd party fraud (e.g. Online). The criminal then uses a network of accounts that they control to distribute the money so that it can eventually be cashed e.g. out at cashpoints; onto prepaid cards; as Western Union transfers etc.

Real-time analysis of the payments data across all payments providers would allow for the mapping of these networks. Different fraud-types may involve different networks. Building and understanding these networks would then allow for:

- Development of predictive algorithms leading to real-time prevention of fraud.
- Revealing active criminal networks, thus enabling the large-scale identification of 'bad' accounts and significant disruption of criminal organisations.
- An invaluable forensics tool for financial institutions and Law Enforcement (LE), leading to greater efficiency (e.g. reporting of financial crime to LE and more efficient investigations)

In addition to detecting and preventing fraudulent activity, transaction analytics can also assist the repatriation of victim's funds when a fraudster is discovered and there are still funds available. This is shown in figure 7 below:

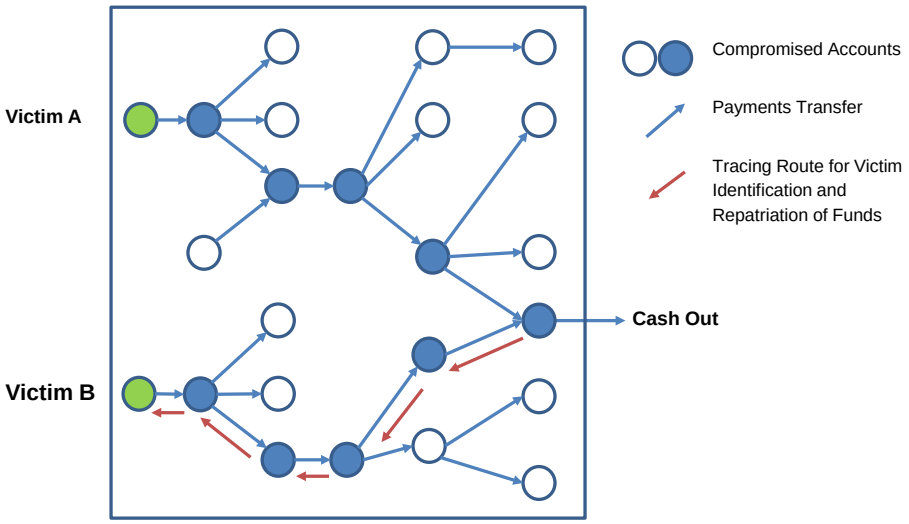

Figure 7 – Funds repatriation example

Once a criminals network of accounts have been mapped, then it will be possible to trace the origin of payments back to additional victims of the APP scam, who are likely to still be unaware that they have been a victim of fraud.

The effectiveness of this analysis was successfully demonstrated in a 'money mule' Proof of Concept commissioned by Financial Fraud Action UK in 2016. In response to this success and the early work by the PSF, a group of PSPs have agreed to fund a tactical initiative to continue the money mule analytics and in addition, to undertake a proof of concept for the funds repatriation analytics. This will generate additional insights for use in the PSF solution as well as providing immediate benefits for consumers.