payments strategy forum

Financial Crime, Data & Security Working Group

Detailed Assessment Phase

V2.0 April 2016

Contents

'To engender user trust in safe and certain payments through collaboratively preventing financial crime.'

1. Executive Summary

APPROACH SINCE FEBRUARY FORUM

In its submission to the February Forum, the Financial Crime, Data and Security Working Group identified four high-priority solution concepts: Identity, Authentication & Risk-scoring; Transaction Data Sharing & Analytics and Financial Crime Intelligence Sharing; Trusted International Ecosystem Registry; Customer Education and Awareness.

The major part of our work since February has been to develop a more detailed assessment of the first 3 of these solution concepts. For each concept in turn, we have held a workshop open to any members of our Working Group and delegates to drive our detailed assessment, including understanding and enhancing the list of relevant known issues and detriments; 'stress-testing' the solution description, to build rigour or identify additional components or features; and identifying achievable benefits, aligned to the detriments.

The output of these 3 assessment workshops has been captured as six potential solution approaches, each summarised below and written up in the detailed assessment document submitted to the Forum.

- Technical Standards for Identify Verification, Authentication, and Risk Assessment
- Payments Transaction Data Sharing And Data Analytics
- Enhanced Payment Transaction Data
- Financial Crime Intelligence Sharing
- Trusted KYC Data Sharing and Storage Repository
- Enhancement of Sanctions Data Quality

For the Customer Education and Awareness priority, we are still in a work-in-progress position. We have taken initial steps to identify a straw-man list of priority campaign topics or messages for different end-user segments, and will build these out further in April and engage with the End-User Needs working group.

In addition in February we identified two other medium-priority solution concepts, which have not been developed in the last five weeks but which are still in the scope for the Working Group to consider further: Consistent Control & Reporting obligations across all payment/ money-transfer providers; and Profiled Control Of Payment Initiation for customers.

Finally, we have identified two other work-streams that will support across all the solution options above:

- Legal work-stream: to pull together an understanding on the existing legal issues or constraints which would need to be addressed in order to enable aspects of these solutions to be viable;
- External Environment work-stream: to identify all the public authorities, industry bodies and industry initiatives, across the financial services arena, that are addressing issues of financial crime.

EMERGING SOLUTION THEMES

The scope for the Working Group covers fraud, money laundering, terrorist financing, bribery and corruption, and sanctions. As we conducted the analysis across our priority solution areas, we identified some common themes that underpin the customer detriments.

- A lack of common formats and standards in specific areas that hinders effective communication between Payment Service Providers (PSPs). E.g. authentication of receiving party, rapid sharing of information on fraud activity across PSPs.

- A lack of an economic business case to address detriments whether individually or collaboratively. E.g. building and monetising a capability for enhanced data with a payment message.
- Acute concerns about current legal and regulatory constraints. E.g. sharing financial crime information between PSPs, due to data privacy, tipping off, Proceeds of Crime Act.
- Loopholes or gaps in the current landscape that enable financial crime activity. E.g. international remittances up to 1,000 Euros can be made in person without an ID check. (Depending on which regulations a PSP acts under, it may not universally be completing Customer Due Diligence (CDD) before it transacts).
- Gaps in capability and infrastructure across different PSPs and in central infrastructures that make it difficult to solve the detriments. E.g. validation of identity documents with Government sources; cross-PSP data analytics to identify fraud and laundering activity (e.g. mule account payments).

SUMMARY OF SOLUTION PROPOSALS

This section summarises the six potential solution approaches identified at our workshops in March

Technical Standards for Identify Verification, Authentication, and Risk Assessment

Many of the weaknesses of the payment systems that are exploited for financial crime are related to the identity of the parties involved. Current solutions and rules are not applied consistently across payment types, across PSPs, and within the whole payment lifecycle. Criminals exploit these deficiencies, harming both individuals and organisations.

The Working Group's solution proposal looks to establish a standard to define and recognise the key capabilities that PSPs need to bring to bear and principles of operation related to identity, including the key principle of a risk-assessment of payment and payment-related transactions.

By establishing basic, end-to-end standardisation, each PSP will be required to document, and in some cases augment, its approach for a set of key capabilities, protecting both payment service users and the integrity of payment systems. Approaches to compliance will vary between PSPs, with smaller organisations having typically a smaller scope and therefore a smaller burden.

This paper also recognises the need of the payment systems for ancillary solutions, both commercial and collaborative, which will give PSPs improved capabilities to manage identity risk in payments.

Payments Transaction Data Sharing and Data Analytics

The UK payment industry creates a very large and high quality data set as a by-product of processing payments through the BACS, FPS and LINK transaction networks. This data set has the potential to provide a multitude of powerful insights that could be used to address many types of financial crime; however to date this opportunity has remained relatively untapped. The emergence of 'big data' analytical capabilities has opened up potential for the industry to better exploit this data set in order to combat financial crime.

This solution approach sets out how this high-quality payments transaction data can be utilised, through the application of big-data capabilities, to address Financial Crime and Anti-money laundering.

To enable transaction data pooling and analytics to address financial crime, the UK industry needs to establish the following capabilities: collaboration and data pooling; data sharing compliance and controls; application of 'big data' capabilities to extract actionable insights; and distribution of insights.

This solution approach provides the ability to address a range of financial crime issues such as identification of money mules, funds repatriation and a risk based approach to intervention.

Furthermore big-data capabilities are flexible and can be applied to an ever-changing range of financial crime use cases, addressing ongoing changes in fraud activities and other financial crime risks.

In any solution based on data sharing, we identify there are significant legal questions to address on privacy and data protection. The Working Group also considers that potential solutions in this field needs to be assessed in the context of the Open Banking initiative to develop open APIs in banking.

Enhanced Payments Transaction Data

Today's financial payment messages follow a number of formats for processing payments for validation, routing and settlement, for both inbound and outbound. FIs are required to process these varied formats and their related metadata to define both the attributes and the data flows required for the payment.

Enhancing the data in payment messages would improve the capability to tackle financial crime by including the following data items (among others):

- identification of payer and payee added to the payment instruction;
- identification of both credit and debit account numbers. For example, by addressing the Account Number structure the use of reference data by some FIs could be avoided;
- identify the purpose of payment or remittance data.

Key benefits this would deliver are greater certainty of the recipient for a payment, real-time fraud risk assessment (e.g. for DWP benefits payments) and lower cost of entry for new, innovative PSPs.

Enhanced payments data can also have wider benefits, providing improved services to end-users and easier access for innovators and new entrants.

Financial Crime Intelligence Sharing

While all PSPs are individually active implementing various measures to combat fraud and money laundering activities, there is an opportunity to enhance cross-PSP interaction to work collectively to safeguard customers. There are however several barriers to making it happen including regulations like data sharing restrictions, tipping off risk, Proceeds of Crime Act.

A number of critical questions from a PSP perspective around intelligence sharing need to be addressed. For example what type of data are PSPs sharing, what do PSPs consider to be intelligence sharing; have PSPs completed due diligence on this data, and is the data worth sharing and valuable? Sensitive data on financial crime activity also needs to be addressed: can PSPs rely on other parties' information, and what are the regulators' expectations?

There are two levels of possible industry co-operation to fight financial crime activities:

- Typology / trends level sharing between various PSPs for AML and fraud.
- Transaction/ customer level sharing and actions between various PSPs, which incorporates:
  - Fraud event response: how PSPs work together to prevent proceeds of fraud being paid away
  - AML suspicious activity, where the combination of suspicion across various PSPs could make a stronger case to assess the money laundering risk of an individual or entity.

Trusted International KYC

Financial institutions (FIs) have to collate and validate KYC information for each customer relationship (e.g. correspondent, corporate, or individual) in order to help address AML and fraud risks. Within an FI the extent of the KYC information processed will vary depending upon the business relationship at

hand and the FI's KYC policy. The implementation of KYC leads to significant duplication of efforts as KYC information collation process must happen for each FI and customer relationship that exists.

The problem is compounded further when considering the international domain where KYC information is needed to mitigate an AML or fraud risk for a customer or beneficiary outside the FI's country footprint.

A KYC Data Sharing and Storage Registry would provide real-time sharing of KYC information between FIs, customers and data providers in order to help mitigate the Financial Crime Risks of all parties. The main capabilities of the solution include firstly a single registry or exchange mechanism (central or distributed) where KYC information may be submitted, exchanged and re-used many times; and secondly the provision of an API gateway where KYC information can be sourced, collated and aggregated from a range of sources both within or outside existing geographies.

If achievable, the use of shared KYC data would improve AML compliance thus benefitting end-users and society overall, and existing PSPs and FIs would be able to realise more systems consolidation and reduce their cost of processing.

Enhancement of Sanctions Data Quality

The quality of the entries on Sanctions Lists directly correlates with the number of alerts raised by Sanctions screening systems. A sanctions list entry with detailed, clean and structured data enables more accurate detection and thus fewer false positives. And conversely, a poor quality entry can cause many false positives that not only result in additional work, but can cause operational problems and unnecessarily delay genuine customer business.

An Advanced Sanctions Data Model has been developed by the UN 1267/1988 Security Council Committee. The rationale driving this model was to enhance the quality of the Sanctions List entries and thus their effectiveness in use. The solution in considered by the Working Group is for HMT to adopt the Advanced Sanctions Data Model.

Adopting this data model for HMT Sanctions would not only enable improved detection capabilities for FIs, but also help eliminate the frequent errors that find their way onto the lists. Promoting the Advanced Sanctions Data Model internationally would aid detection quality domestically, and also help the transfer of Sanctions Entity information between states.

Customer Education and Awareness

A priority issue in Financial Crime is the ability of end-users to identify and understand how criminals seek to exploit end-users in order to obtain or launder money, and the steps end-users should take to reduce the risk of becoming a victim or unwitting participant in financial crime. Obtaining personal data about customers is the most valuable asset in the financial crime market because it enables access to customers' financial relationships. Awareness and education will not totally resolve this issue, but placed alongside other measures they can have a substantial impact on customers' abilities to mitigate the risks.

The Forum's approach to Education and Awareness will clearly be informed by the End-Users Needs working group alongside our financial crime perspective. These campaigns will need to target customers in many different segments and sub-groups, across consumers, businesses, charities, and public sector.

NEXT STEPS

Our view of the next phase for the Financial Crime Working Group is summarised here.

- For the six solution options covered in this report, developed in detail in the period since February's Forum, the Working Group recommends a further phase of detailed analysis to move from a potential approach towards practical recommendations. As part of next steps in defining the solutions, we will further develop a use-case requirements perspective, building on the detriments and issues the working group has captured.
- For Customer Education and Awareness, we will work to align with the End User Needs WG and to identify stakeholders in the industry that the Forum will need to engage with to pursue its campaign priorities.
- A key activity we envisage is that the working groups should identify common issues and work closely, across the Working Groups, on developing the next level of analysis and proposal. Issues that require a common approach include Identify, Verification & KYC; Enhanced Payments Data and Standardisation; and Customer Education and Awareness.
- We will further progress our activities and deliver next-phase outputs for four other (medium-priority) work-streams in the Working Group.
- The Working Group recognises the need to engage on financial crime issues with a broad set of financial services stakeholders beyond the direct payments community, to draw up an effective set of recommendations and delivery approaches. This will be part of our External Environment activities.

2. For discussion

[Highlight any areas you wish to discuss / reach agreement on at the Forum]

1. Plan for the period from mid-April to end-May, a key period for further analysis leading up to the June Forum
   - the level of further analysis required for the strategic recommendations & priorities: benefit & cost analysis; options for delivery approach (who, how); funding model;
   - the right level of co-ordination between the 4 working groups, balanced with each working group continuing to drive its own analysis and recommendations ;
   - the plan for the work of the independent consultants and how this will be aligned with further work of the Working Groups.

2. For Financial Crime recommendations: Buy-in from the wider financial services community ahead of the consultation document, such as the approach to engage other Financial Services bodies / initiatives – for example (among many) alignment with Joint Fraud Taskforce; Serious & Organised Crime Financial Sector Forum (and Joint Money Laundering Intelligence Taskforce (JMLIT)).

3. Joint approach across Working Groups for 'customer education and awareness' recommendations by the Forum – and for engagement with wider industry programmes and priorities.

4. Discussion on any potential impact of the EU referendum result, a few weeks before the consultation document. Specifically, do the Forum's recommendations have any dependence on the Stay/Leave decision?