payments strategy forum

Financial Crime, Security and Data Working Group
Triage and Prioritisation Analysis

1. Executive Summary

During December, the Working Group gathered input from its members on the problems for financial crime that exist in and around the payments systems, and customer detriments that result from these. Members were encouraged to submit use-case scenarios to demonstrate the real-life impact of these issues.

We held a 2-day workshop on 14-15 January for experts proposed by the Working Group. The workshop firstly reviewed and enhanced the issues/detriments identified, then grouped these into major themes for the Group to address. The workshop then identified solution ideas to address the issues identified in each theme; nine solution ideas were developed. The workshop finished by providing an initial view of the prioritisation of these solution ideas for collaborative projects by the payments industry.

Since the workshop each solution idea has been written up into a 'solution concept' description (2-3 pages) which in turn has enabled the Working Group to further consider the prioritisation of these at its meeting on 22 February. The solution concepts we are proposing for progressing to the next stage for detailed analysis are:

- 'Identity, Authentication and Risk-scoring'
- 'Transaction Data Sharing and Analytics', ...incorporating
    - 'Centralised Capability for Financial Crime Data Modelling'
    - 'Business architecture & governance for Data Sharing'
    - 'Financial Crime Intelligence Sharing'
    - 'Risk-based approach to Intervention'
- 'Trusted International Ecosystem Registry'
- 'Customer Education on Financial Crime'

Our next steps are to move into detailed assessment for these solution concepts:

- Develop the solution definition to more detail, and carry out quantitative cost-benefit analysis;
- Pursuing a full dialogue with relevant stakeholders to challenge the assessment and build support for the proposals;
- Assess and agree the approach for 'medium priority' solution options identified;
- Ensure ongoing alignment to priority detriments identified.

2. Call to action

The Forum is asked to consider this update and confirm the solution concepts that are proposed for the detailed analysis stage.

3. Triage and prioritisation analysis

As per the high level work programme and evaluation framework discussed and agreed at the December Forum, the **Financial Crime Working Group** has been through an exercise of assessing its long list of detriments. This section provides our high level analysis for Forum consideration before we progress to the detailed assessment.

3a. Detriment grouping and definition

Original detriment(s) *(taken from foundation document agreed at the December Forum):*

- On-line security measures have technical problems and are too complicated for consumers – this is leading to high rates of sale-abandonment.
- The current decentralised KYC / Fraud / AML / sanctions model incurs high costs and makes compliance expensive for small indirect PSP's and end users.

Grouped / Refined / Defined

Customer identity, authentication, and knowledge

Customer perspective - Detriments

- An identity is used successfully by a criminal (3rd-party)
- Day-to-day concern about risk of identity theft, risk of fraudulent activity on an account
- A payment is made to a wrong account
- Friction in the payment experience, e.g.
  - Online payment verification checks (e.g. a '3D-Secure' retailer)
  - Point-of-Sale card payment declined by PSPs fraud systems (as a 'false positive')
  - Opening a bank account, application is declined due to ID checks
- Businesses pay into accounts not owned by their suppliers due to false invoices, false change of bank account notifications

Industry perspective

- Understand who is the payment initiator (payer) and paying account
- Understand who is the payment recipient (payee) and the beneficiary account
- Current ID solution may not be sufficient for proof of identity in criminal cases
- Know who are vulnerable customers
- At account opening, where customers are seeking access to payments instruments, understand who is the applying customer

Original detriment(s) *(taken from foundation document agreed at the December Forum):*

- The current decentralised KYC / Fraud / AML / sanctions model incurs high costs and makes compliance expensive for small indirect PSP's and end users
- Consumer data is exposed to theft at multiple points along the value chain, leading to increased fraud costs.
- Unlimited Direct Debit Guarantee is open to fraud

Grouped / Refined / Defined

Data Sharing, Reference Data, Analytics

Insufficient reference data and lack of knowledge share results in gaps in preventing financial crime: fraud, money laundering, terrorist financing, bribery and corruption.

Customer perspective

Real-time payment risk assessment is limited, reducing the capability of customers and PSPs to act against fraudulent payments. For example business customers and Government departments are constrained in identifying fraud by the lack of information available on the payee/ beneficiary account, and the payer/ remitter account.

Switching to a new bank means re-doing checks for KYC, anti-money-laundering (AML), anti-terrorist-financing.

When customer realises a payment is actually a fraud, banks cannot work quickly together to target mule accounts and to prevent funds being paid away.

Industry perspective

Banks cannot make fully reliable risk decisions on 3rd-parties as they cannot be 100% sure of identity and information about them

The beneficiary bank has limited information about the remitter, the reason for payment, the network of accounts that the beneficiary account transacts with – impacting its ability to identify accounts used to receive proceeds of fraud.

Banks cannot comply easily with KYC, AML, anti-terrorist-financing requirements on their own customers, or on 3rd-parties.

Unnecessary bank secrecy prevents effective control of money laundering.

Original detriment(s) *(taken from foundation document agreed at the December Forum):*

- Difficult for users to make international payments with respect to identity assurance as remitters and beneficiary details need to be checked for sanctions (payments filtering)

Grouped / Refined / Defined

International payments and account activity

Customer perspective

Lack of clarity of the speed, costs and risks of international payments.

Bank account access – opening or maintaining account facilities – regulatory burden is different, and variable, in different territories (AML)

Perceived risk of fraud is higher for international payments; e.g. businesses pay into accounts not owned by their suppliers due to insufficient ability to confirm payee identity and beneficiary account

Industry perspective

Customer identity and Data sharing approach for international payments is less robust that for UK-UK payments.

Lack of understanding of ultimate beneficiary owner (UBO) and robustness of KYC.

Emergence and growth of alternate PSPs and methods where regulation is less robust, banks have limited control.

- e.g. block chain,
- cross border payments being made under the disguise of domestic payments ('Hawala'-type payments), give consumer safety issues, and money laundering opportunities

Name of legal entities or individuals is not sufficient to uniquely identify them across jurisdictions

Original detriment(s) *(taken from foundation document agreed at the December Forum):*

- Merchants have little information on fraud levels and no appeals process for card scheme fines
- Card scheme rules need to be localised
- Unlimited Direct Debit Guarantee is open to fraud

Grouped / Refined / Defined

Payment scheme issues/ weaknesses

Customer perspective

Insufficient merchant education and understanding on fraud levels, and best practice for engaging with Payment Schemes

NB: the BACS scheme is reviewing the Direct Debit guarantee as part of its strategy update

Grouped / Refined / Defined

Customer Education & Awareness

Customer perspective

Lack of customer awareness about mule accounts:

- For avoiding 'non-complicit' involvement
- Criminal implications of complicit involvement

Lack of customer awareness of widespread methods use for fraud ("MO's": 'modus operandi') – such as duped customer payments (e.g. caller requesting remote access to PC; romance scams; pension liberation; invoice diversion; ghost payroll; etc)

3b. Orphan detriments

- Detriment: "Consumer data is exposed to theft at multiple points along the value chain, leading to increased fraud costs.
  - The Working Group considers this issue as broader that the payments industry's payments systems and processes. This issue relates to all organisations (e.g. retailers, utility service providers) holding customer payment details, and is fully covered by the scope of the Data Protection Act. It is a vital consideration for an overall strategy to reduce fraud. The Working Group will keep this in mind for its Customer Education solution approach, but considers this detriment is equally important for the User Needs and Horizon Scanning working groups to be considering strategic, longer term requirements and solutions.
- Detriment: "Merchants have little information on fraud levels and no appeals process for card scheme fines"
- Detriment: "Card scheme rules need to be localised"
  - The Working Group is continuing to consider these two detriments to understand whether these issues should be flagged to the card schemes to consider directly in their scheme processes and governance across acquirers, merchants and users; or whether these are issues that could be addressed collaboratively via this initiative's priority actions.

3c. Triage and prioritisation

Grouped detriment	Potential Solution(s)			High level CBA (+ / -)	Priority (HML)
	Solution already available or under development (Y/N)	**New** *(Capture the solution at a high level, please note this doesn't have to be a technical solution, could be education; rules changes etc.)*	**Potentially Requires collaboration (Y/N)**		
Customer identity, authentication and knowledge	Y	Identity, Authentication and Risk-scoring	Y	*(next phase)*	H
Data Sharing, Reference Data, Analytics	Y	Transaction Data Sharing and Analytics *…incorporating*	Y	*(next phase)*	H
	Y	Centralised Capability for Financial Crime Data Modelling	Y		
	Y	Business architecture & governance for Data Sharing	Y		
	Y	Financial Crime Intelligence Sharing	Y		
	Y	Risk-based approach to Intervention	Y		
International payments and account activity		Trusted International Ecosystem Registry	Y	*(next phase)*	H
Customer Education…	Y	Consumer Education on Financial Crime	Y	*(next phase)*	H
All		Consistent Control & Reporting obligations across all payment/ money-transfer providers	Y		M
Customer identity, authentication and knowledge		Profiled control of payment initiation for all customers	Y/N		M