Counter fraud and the Open Banking Ecosystem

Date: January 2018
Version: 1.0
Classification: PUBLIC

With thanks to our contributing organisations

Bank of Ireland

Barclays Bank

Danske Bank

Financial Fraud Action UK

HSBC Group

Lloyds Banking Group

Nationwide

PayM

Royal Bank of Scotland Group

Santander

Contents

Executive summary

This document details the counter fraud approach that will protect the Open Banking Ecosystem and mitigate the risks arising from fraudulent activity. It has been developed and approved by members of the Open Banking Counter Fraud Strategy Group (CFSG).

The counter fraud approach abides by the IT Security Principles that were approved by Implementation Entity Steering Group (IESG) in 2016:

- The service will be highly available and highly secure
- The Information Security risk appetite is very low
- The service must engender customer confidence and trust
- Decisions will be risk based
- Security must be embedded in all aspects of the solution

This approach does not define counter fraud policies or processes for Participants. These remain the responsibility of each Participant involved in delivery of open banking transactions.

In the Autumn Budget on 22 November 2017, the Chancellor of the Exchequer announced an expansion of the Open Banking Implementation Entity scope[1]. The Open Banking Implementation Entity will undertake a further threat analysis of the additional scope in Q1 2018 with a view to implementing mitigating actions.

The Counter Fraud Approach details the steps taken by the Open Banking Implementation Entity and Participants to identify, assess and mitigate identified fraud threats. These steps are split into the areas of:

[1] https://www.openbanking.org.uk/wpcore/wp-content/uploads/2017/11/FAO-CMA_Proposed-Amendments-to-Agreed-Arrangements_v_final.pdf

Prevention	Detection	Response
• Open Banking security profile • Application security • Education & good practice • Operational controls • API risk indicators • Participant fraud controls	• Participant enrolment • Security operations • Information and intelligence sharing	• Revocation • Liability model • Dispute management system

The counter fraud approach also details additional actions that will be scoped and assessed for viability in 2018:

1. Use of data and analytics
2. Operational risk management capability
3. Machine based learning
4. Co-ordinated response across Participants
5. Crisis response

Implementation of many of these actions falls outside the Open Banking Implementation Entity scope – scoping and viability assessment will be undertaken by the Open Banking Implementation Entity with a view to implementing in the appropriate organisation once approved by the IESG.

1 BACKGROUND & CONTEXT

Fraud is defined by the Fraud Act as an act (of intent or omission) carried out with the purpose to “make a gain for himself or another or to “cause a loss to another or to expose another to a risk of loss”. Fraud can take many forms and is acknowledged to be impossible to eliminate. The recent introduction of innovative technology and payment methods has increased the opportunities for bad actors to instigate financial fraud in the UK. Traditional methods of fraud (such as money laundering) have become easier to instigate and have been joined by new methods such as impersonation and computer insertion. The values associated with financial fraud are a significant drain on financial institutions, consumers and the UK economy.

Financial fraud losses arising from remote payments, credit cards and cheques totalled £768m in 2016 which represented an increase of 2% on 2015 (following a 26% rise in 2014). A further £1.38bn of financial fraud was prevented[2]. The National Crime Agency (NCA) estimates that total fraud losses in the UK could be as much as £193bn and UK residents are more likely to be victims of fraud than any other crime. Corrupt individuals working in financial institutions are key enablers to fraud whilst the use of malware and phishing is a key driver[3]. 'Card not present' fraud carries an inherently higher risk of fraud, with losses increasing by 9% in 2016 to £432.2m. This was primarily due to use of card details stolen through data loss, phishing (email) and smishing (text message) activity.

The development of APIs for secure sharing of customer information could increase opportunities for financial fraud which will need to be managed and mitigated effectively by Participants. For example:

- The introduction of new types of regulated payment services could increase the likelihood of security breaches and data losses leading to either direct fraud losses or a fraudulent approach on another channel

- Fraudsters are increasingly using social engineering (phishing – email, vishing – phone, and smishing – SMS messages) to gain access to customer information and enable fraud

- The increased use of technology can increase the ability to perpetrate fraud against individuals – through spoofing of phone numbers and email addresses to persuade victims to share confidential or personal information

- The use of opaque business structures could be used to circumvent anti-money laundering measures using third party providers to break the trail of the laundering process

Several external studies and articles relating to open banking have identified fraud and the risk of fraud as a key barrier to take up of new payment services by Payment Services Users (PSUs). A robust approach to fraud from all Participants is critical to ensuring successful implementation of the programme.

[2] Fraud The Facts 2017 – The definitive overview of payment industry fraud, FFA UK, 30 March 2017

[3] National Strategic Assessment of Serious and Organised Crime 2017, National Crime Agency, 28 June 2017. The language used here is that of the NCA report – corrupt actors are considered threat actors and key drivers of fraud are threat vectors in the OB risk assessment.

2 SCOPE OF THE COUNTER FRAUD APPROACH

The Counter Fraud Approach addresses fraud risks that arise between Participants (the Open Banking Triangle of Trust). There is also a risk of fraud within open banking transactions being invisible to the Open Banking Implementation Entity and poorly co-ordinated across Participants and PSUs. Consequently, additional activity is identified which could mitigate fraud across the ecosystem – and provide a level of protection for PSUs and SMEs. Implementing this activity is beyond the scope of the Open Banking Implementation Entity; the role of the Open Banking Implementation Entity is limited to scoping and assessing potential options for implementation.

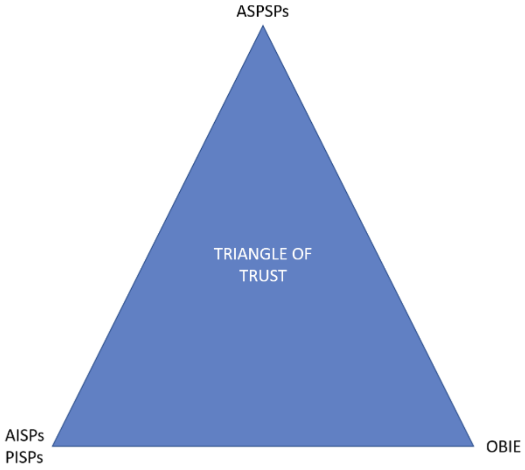

Fig 1 the Open Banking Triangle of Trust

The CFSG agreed that the approach needed to address the areas of: Technical Barriers & Solutions, Policy & Processes and Education & Communication. This supports safe and secure implementation of the Open Banking Ecosystem and forms part of the security approach to open banking transactions.

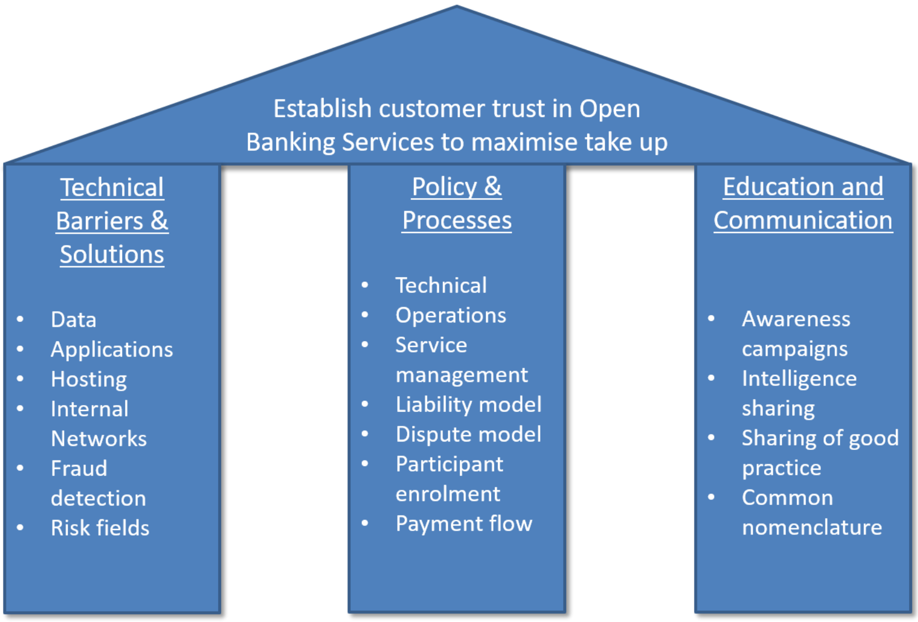

Fig 2 Counter Fraud Approach Scope

3 APPROACH

The Open Banking Implementation Entity Information Security Working Group (ISWG) agreed in early 2017 to create the CFSG which focusses specifically on counter fraud measures. This group drew on Open Banking Implementation Entity stakeholders for membership and held its inaugural meeting on 21 February 2017. The group meets regularly and undertakes the following activities:

- Review and assessment of Open Banking Implementation Entity proposals from a counter fraud perspective
- Analysis and feedback on proposed solutions
- Threat analysis of the Open Banking Ecosystem
- Development of a counter fraud approach to mitigate and manage identified fraud threats

All counter fraud strategies consist of three main components, which combine into mechanisms which deter fraud:

1. Prevention – measures designed to stop fraud occurring in the first instance
2. Detection – measures to identify fraud when prevention measures have failed
3. Response – measures to respond, mitigate and resolve identified fraud

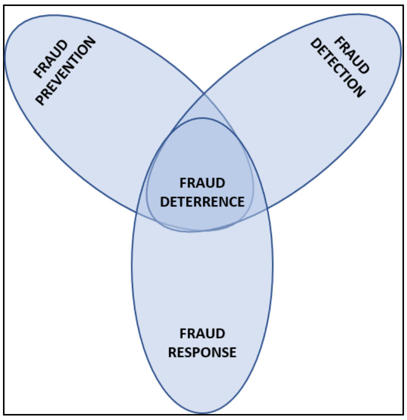

Fig 3 Counter Fraud approach components

4 COUNTER FRAUD PRINCIPLES

The following principles guide the Open Banking Implementation Entity Counter Fraud approach:

- PSD2 and PSR alignment
- Use or amend existing processes and approaches where possible
- Prevention, Detection and Response
- Continuous improvement throughout live services
- Majority agreement is sufficient for a recommendation to the programme
- Does not create barriers to entry for Participants
- Risk based approach
- Proportionate to potential threat and impact
- Risk appetite and fraud policy sits with the institution

5 IDENTIFIED THREATS

The CFSG reviewed the epics and stories in Confluence produced by the Open Banking Implementation Entity programme team for the 2018 launch. In May 2017, the Open Banking Implementation Entity and Fighting Financial Fraud Action UK (FFA UK) held a joint workshop which identified potential new or increased threat surfaces. Further workshops and meetings examined and assessed the threats before allocating them to the different classes of Participants involved in the Open Banking Ecosystem. Although no new fraud threat surfaces were identified, the group considered that access to account data and payment transactions could increase the threat surface and opportunities for fraudulent activity.

The likelihood and impact of individual risk varies depending on the device and technology used to transact using an Open Banking API – which adds complexity to the effectiveness of any mitigation activity. The transition period between implementation of the CMA order and Payment Services Directive II (PSD2) and the introduction of PSD2 Regulatory Technical Standards (RTS) could increase the potential for fraud. This is because consumers of open banking and PSD2 transactions will operate in a mixed environment of sometimes sharing their banking credentials (without an Open Banking API) and authorising transactions directly with their ASPSP (using Open Banking APIs). This counter fraud approach therefore addresses the fraud threats in operation at the launch of the Open Banking Ecosystem in January 2018 – and will adapt to changing circumstances as new products, services and requirements become available.

5.1 Fraud threats within the scope of the Open Banking Implementation Ecosystem

Most of the identified fraud threats originate from the introduction of new types of regulated payment services which have the potential to increase fraud risks for consumers using these services. The Open Banking Implementation Entity is protecting its systems and processes – notably the Directory and its enrolment processes. Open Banking Participants have counter fraud policies and processes in place to address risks within their operations and sphere of influence.

Without ongoing monitoring, management and mitigation of these risks, there is a risk of reduced transformation of the UK banking sector from greater competition and innovation. The next stage of this approach proposes to focus on the consumer[4] fraud threat in open banking transactions (both payment initiation and account information) and to identify potential mitigating actions to reduce this.

6 FRAUD PREVENTION

Fraud prevention employs techniques to stop fraud from occurring, although it is widely accepted that no single fraud prevention technique will be wholly successful. The Open Banking Implementation Entity fraud prevention techniques are layered with those from other parties:

[4] In this instance the 'consumer' includes both individuals and businesses.

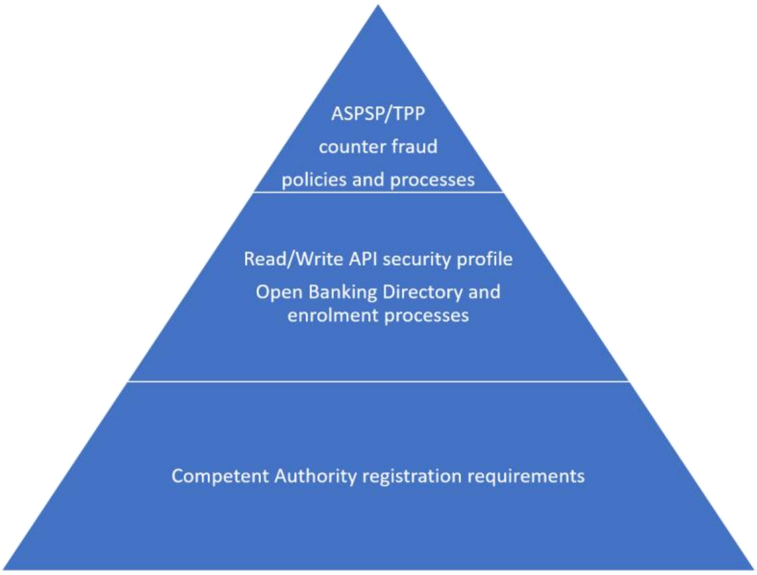
ASPSP/TPP
counter fraud
policies and processes
Read/Write API security profile
Open Banking Directory and enrolment processes
Competent Authority registration requirements

Fig 4 The Open Banking Implementation Entity fraud prevention in context

Fundamentally, open banking transactions from all providers are based on technical solutions - and use technology to increase competition in the UK banking sector. The use of APIs and cloud based services can increase threat surfaces and the likelihood and impact of fraudulent activity. A significant element of the Open Banking Implementation Entity fraud prevention therefore uses technical barriers – developed by the Open Banking Implementation Entity into an agreed security profile.

6.1 OB Security Profile

The Open Banking Implementation Entity security methodology takes a layered approach to security, ensuring that security is designed into the APIs and messaging flows. The security profile is designed to ensure that all Participants can transact in a safe and secure manner, using common protocols.

The Open Banking Implementation Entity security profile defines how the Read/Write APIs are securing using a multi layered approach. The OAUTH 2.0 authorisation framework, and Open ID Connect identity authentication protocols are layered over Mutually Authenticated Transport Layer Security (MATLS) to provide a robust and secure security profile. The security profile is published on the Open Banking Implementation Entity website at https://www.openbanking.org.uk and contains details on:

- Open Banking Security Profile
- Security Architecture
- JSON Security Suite Information
- Implementation Guide

The Security Profile also uses the OpenID Foundation's Financial API Read and Write (FAPI) API Security Profile. This specification is published on the OpenID Foundation website at openid.net.

The Open Banking Implementation Entity is a member of the OpenID Foundation, a non-profit international standardisation organisation of individuals and companies committed to enabling, promoting and protecting OpenID technologies. The Open Banking Implementation Entity is working with the OpenID Foundation to ensure that the profile is maintained as a world class security standard which provides the very best protection available for all users.

6.2 Application Security

The Open Banking Implementation Entity runs on a 'cloud first' approach utilising industry standard software-as-a-service applications. Every application has native security built into their delivery model and are also protected by Denial of Service (DDoS) protection and a Web Application Firewall (WAF). The Open Banking Implementation Entity has undertaken progressive penetration testing since November 2016 and has a regular programme in place to ensure ongoing threat identification and mitigation.

The core of the Open Banking Ecosystem is the Directory – which provides a 'whitelist' of Participants enrolled with the Open Banking Implementation Entity. The Directory maintains Participant data, provides a digital identity for an enrolled Participant and creates software statements for each application that utilises the Open Banking APIs. The Directory and transactions are secured using root PKI certificates.

The in-house development team includes embedded security architects and Identity and Access Management experts. All applications are regularly assured by both internal and external application security experts. The ISWG has signed off the assurance approach and provided a set of assurance requirements to the Open Banking Implementation Entity. This methodology ensures that the Open Banking Implementation Entity is constantly reviewing and refining its approach in line with requirements from Participants and industry best practice.

6.3 Education and good practice

All fraud threat analysis identifies people as the weakest link in any process or interaction. Given the potential for open banking to lead to both monetary loss and data breaches, the CFSG quickly identified that good practice guides to prevent fraudulent activity were of value. There are many organisations already producing material and the purpose of the Open Banking Implementation Entity guidance is to build on existing material to make it relevant to open banking products and services. The wide number of stakeholders supporting the Open Banking Implementation Entity has been beneficial in producing these guidance documents.

The counter fraud good practice guide can be found on http://www.openbanking.org.uk and is designed to be read alongside the Information Security good practice guide to support a secure and safe open banking environment.

6.4 Operational Controls

The ‘Insider Threat’ of fraud can be accidental (a mistake) or malicious (intentional). Corrupt individuals working within banks are considered by the NCA to be a key enabler of fraud[5]; it is reasonable to extend this in the context of open banking. All Open Banking Implementation Entity workers are vetted during the recruitment process and robust management processes are in place and regularly reviewed.

6.5 API Risk Indicators

Following feedback from the ISWG as well as the CFSG, several risk indicators were included in the Open Banking Implementation Entity Read/Write APIs. Whilst these do not remove the need for each ASPSP to undertake their operational fraud risk activity, they provide additional contextual information that can support internal ASPSP fraud prevention and detection processes.

6.6 Participant Fraud Controls

All ASPSPs have established successful fraud operations teams identifying, managing and mitigating fraudulent activity within their operating environments. It is outside the scope of this approach to detail or suggest policies and processes that Participants should adopt for their organisations.

The CFSG fraud threat analysis and the Open Banking Implementation Entity mitigations have enabled existing counter fraud teams to identify potential changes to their risk profile that they will be facing once the Open Banking APIs are a live channel for their customers. Responsibility for adapting to those changes and mitigating the risks sits within each organisation to manage in line with their risk profile and appetite.

ASPSPs should ensure that access to payment accounts to TPPs is provided without discrimination. This must enable sufficient account access to allow the TPP to perform the service which the PSU has requested. It is possible for ASPSPs to deny access to a TPP - based on objective and non-discriminatory reasons such as suspicion of fraud. When denying access, ASPSPs must notify the FCA or their relevant regulator.

The Open Banking Implementation Entity APIs involve a ‘redirection model’ - which means that the PSU is authenticated in the domain of their ASPSP for payment initiation or account information transactions. Existing ASPSP fraud prevention and detection engines will continue to be utilised to ensure transaction requests are genuine. Should a PSU fail to authenticate themselves at the ASPSP, a transaction request would be declined in line with policy of the ASPSP.

[5] National Crime Agency – Strategic Assessment of Serious and Organised Crime, 2017

The CMA Order[6] requirement for a ‘whitelist’ of Participants, which is achieved through the Directory enrolment process, provides additional certainty that Participants are appropriately regulated.

7 FRAUD DETECTION

Fraud detection occurs when fraud prevention has failed and aims to identify fraud as quickly as possible. Fraud detection is continuously required as it is unlikely that organisations or individuals will be aware that fraud prevention techniques have failed. It is important that both the Open Banking Implementation Entity and Participants take measures to prevent fraud. Equally importantly, strong detection methods are required to identify the fraud as soon as possible. As fraud vectors are continuously evolving, fraud detection methods must also evolve.

7.1 Participant Enrolment

The CMA Order requires whitelisting as a system for the approval of TPPs to participate in the Open Banking Ecosystem. Open Banking Participants are required to enrol onto the Directory. Once enrolled, Participants will receive digital certificates and be able to create software statements that will enable trusted transactions in the open banking ecosystem.

The Open Banking Implementation Entity enrolment process includes a check against relevant competent authority registers to ensure that Participants have the appropriate regulatory permissions. The Open Banking Implementation Entity has additionally engaged a specialist provider to undertake identity verification checks to ensure that individuals are who they say they are, and are authorised to enrol on behalf of the entity they claim to be associated with. Following review from the OB Support Services Working Group (SSWG) and endorsement from the ISWG and Regulatory & Legal Working Group (RLWG), these checks are based on known standards and processes equivalent to levels that meet civil court requirements. The Open Banking Implementation Entity has used the approach outlined in the UK Good Practice Guide 45 (GPG45) in accordance with Level of Assurance 2 (LOA2) as the basis for specifying this service. Further information can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/370033/GPG_45_identity_proofing_v2_3_July_2014.pdf

The Open Banking Implementation Entity also validates the link between an individual and an organisation prior to going live with the full service on 13th January 2018. This aligns to the joint CESG/Cabinet Office Good Practice Guide 46 – Organisation Identity.

[6] The Retail Banking Market Investigation Order 2017, Part 2,10.2.3*c)

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/271278/Good_practice_guide_organisation_identity.pdf

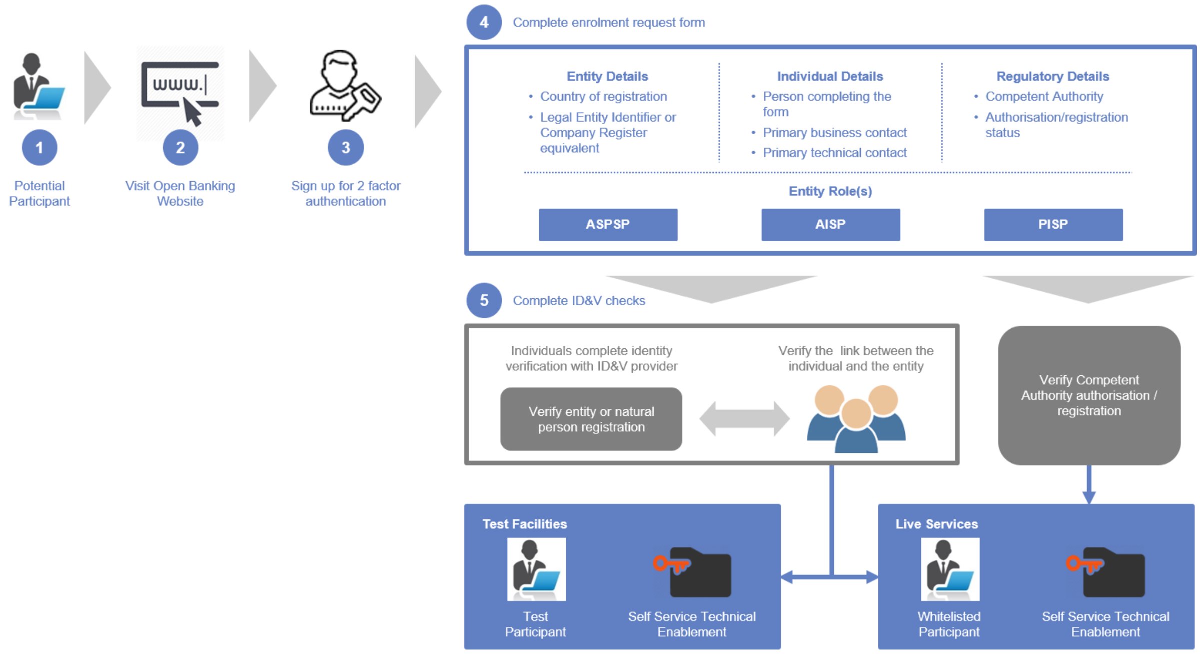
1
Potential Participant
2
Visit Open Banking Website
3
Sign up for 2 factor authentication
4
Complete enrolment request form
Entity Details
• Country of registration
• Legal Entity Identifier or Company Register equivalent
Individual Details
• Person completing the form
• Primary business contact
• Primary technical contact
Regulatory Details
• Competent Authority
• Authorisation/registration status
Entity Role(s)
ASPSP
AISP
PISP
5
Complete ID&V checks
Individuals complete identity verification with ID&V provider
Verify the link between the individual and the entity
Verify entity or natural person registration
Verify Competent Authority authorisation / registration
Test Facilities
Test Participant
Self Service Technical Enablement
Live Services
Whitelisted Participant
Self Service Technical Enablement

Fig 5 January 2018 Participant enrolment process

7.2 Security Operations

In February 2017, the Open Banking Implementation Entity Information Security team defined the requirement for a security operations centre (SOC) that was supported by a security incident and event monitoring (SIEM) solution. The SIEM takes log feeds from all Open Banking systems and uses automated learning alongside predefined use cases to identify security incidents and anomalous behaviour. Some of these security incidents will be attempted fraud or attacks on the Open Banking Implementation Entity's systems to perpetrate fraud. Incidents and events will be investigated and reported. When combined with Information and Intelligence Sharing, this data and analysis will be of benefit to the Open Banking Ecosystem and Participants.

7.3 Information and Intelligence Sharing

Financial Fraud Action UK (FFA UK) already has an established membership model for sharing information and intelligence relating to fraud in UK financial institutions. This benefits from sharing of knowledge and good practice across members as well as identifying new and emerging threats from the data provided. In 2018, FFA UK aims have a membership model that is open to TPPs as well as ASPSPs and provide services that relate to open banking transactions.

In addition, Participants will have the opportunity to participate in regular fraud calls for a limited period following the launch of the Open Banking Ecosystem on 13th January. The duration of this service will be determined by Participants on an iterative basis.

Beyond the launch of open banking transactions, Participants will be able to benefit from existing FFA UK services – sharing data via the Financial Intelligence Sharing Service (FISS), comparing performance to peer organisations (from anonymised data) and access to regulators and law enforcement agencies to respond to fraudulent activity on an industry basis.

8 FRAUD RESPONSE

Strong fraud prevention and detection techniques also require strong responses to fraud combine into an environment that deters perpetrators of fraud. The Open Banking Implementation Entity has several response techniques that create fraud deterrence.

8.1 Revocation

The Open Banking Implementation Entity may only revoke access to the Directory when the relevant competent authority has revoked the regulatory status of a Participant and this appears on their register. A Participant can also request voluntary withdrawal from the Directory. Use cases have been developed and built into the Directory release for 13th January 2018 to reflect these scenarios. Revocation will be undertaken in line with Service Level Agreements approved by the IESG.

8.2 Liability Model

Liability in the open banking ecosystem is generally governed by the liability model as described in the Payment Service Regulations (PSRs). In addition, the Open Banking Implementation Entity has developed a recommended dispute management system which has just launched.

8.3 Data breaches

Liability for data breaches is defined in the Data Protection Act 1998 and from May 2018 with the applicability of the General Data Protection Regulation (GDPR) and other associated legislation.

8.4 Financial fraud and unauthorised transactions

The Payment Services Regulations clearly stipulate that in the circumstances where a PSU identifies an unauthorised transaction (which could include fraud) the ASPSP must immediately refund the PSU. The ASPSP can decide whether to pursue a claim against the TPP for the amount that was refunded to the PSU. Participants will be encouraged to use the Open Banking Implementation Entity approach to dispute management to resolve issues pragmatically and quickly.

8.5 Dispute management system

The option to resolve economic loss via legal action is costly and time consuming. The Open Banking Implementation Entity has therefore developed a voluntary dispute management system which will provide a pragmatic approach to managing issues between Participants.

The model is in two phases:

- *Phase One*: a proposed mechanism for a standard communication protocol between all involved ASPSP(s) and TPP(s). This is facilitated by paper based forms and specifications for completion and maintenance of details of complaint/dispute handling contacts at each participating entity. This is aimed at allowing for an early resolution between all parties involved.

- *Phase Two*: An escalation process which encompasses the existing Financial Ombudsman solution and is looking to define a suitable substitute for the Financial Ombudsman where the dispute is outside their remit (i.e. not related to an individual/microenterprise) to facilitate resolution ahead of any need for legal action whilst not removing that option from any party should they so wish.

9 FURTHER MITIGATIONS FOR FUTURE INVESTIGATION

The Open Banking Implementation Entity has ensured that strong counter fraud defences and security are at the core of its solution. The timeline for implementation of the CMA remedies was extremely challenging and several further techniques will be examined and assessed during 2018 for potential application within the Open Banking Ecosystem. Furthermore, the expansion of the Open Banking Implementation Entity scope announced in November 2017, introduces additional deliverables that will require a fraud threat analysis and potentially additional counter fraud measures.

Many of these solutions will be readily available and require limited adaptation for transactions within the open banking ecosystem. Some are outside of the Open Banking Implementation Entity scope; in these instances, the Open Banking Implementation Entity role will be scoping and analysis of potential implementation options.

9.1 Data and Analytics

The development and introduction of big data and big data analytics tools could be of value to countering fraud within the Open Banking Ecosystem. More recent developments such as user behaviour and predictive analytics mean that having the capability to analyse transaction and fraud data can lead to valuable insight to emerging threats and attacks to the benefit of all Participants.

Implementing this is outside the scope of the Open Banking Implementation Entity and an external organisation is more likely to have the capability and capacity to co-ordinate across different interested parties. Work will be undertaken in 2018 to explore the potential for the use of data analytics to monitor and analyse fraud. The CFSG has already identified potential partners in this area.

9.2 Operational Risk Management Capability

No counter fraud approach will completely eradicate fraud – and new threats and threat actors will be emerging as open banking services develop. The Open Banking Implementation Entity is also developing further functionality which could introduce new fraud threats and require ongoing risk management capability to identify and respond to new fraud risks.

There are some simple operational activities that the Open Banking Implementation Entity can undertake to build further fraud prevention and detection into its operations:

- *Membership of Cifas and FFA UK* – these organisations provide shared information and intelligence relating to known and suspected fraud. Cifas is a non-profit organisation that hosts cross-sector fraud databases and provides services relating to UK bank account holders and vulnerable people.

- *Use of an anti-phishing detection service* – a common fraud vector is phishing - where a fraudulent party impersonates a legitimate organisation. Many third parties provide services to detect and takedown organisations falsely impersonating the Open Banking Implementation Entity. When combined with membership of an organisation such as Cifas, information could be shared with other parties to prevent fraud elsewhere.

- *Implementation of Domain-based Message Authentication, Reporting and Conformance service (DMARC)* – DMARC protects against domain name spoofing and can be used to detect against unauthorised email activity and automatically block or discard them in accordance with the Open Banking Implementation Entity Information Security policy.

9.3 Machine Based Learning

Although the Open Banking Implementation Entity does not undertake any PSU transactions, the entry point to the Directory remains a potential weakness within the Ecosystem. As the Directory becomes more mature and the nature of fraud risks clearer, the Open Banking Implementation Entity should identify and scope potential fraud detection activity that could be built into the Directory enrolment and Identity and Access Management (IAM) solutions and monitored via the Open Banking Implementation Entity SIEM. Machine based learning and behavioural analytics are two of the tools that will be assessed and reviewed for applicability to the Open Banking Implementation Entity technical implementation.

9.4 Co-ordinated response across Participants

It is unlikely that fraudsters will target customers of only one ASPSP – meaning that some level of co-ordination in responding to detected fraud will be required. This is likely to combine many of the techniques outlined above but also needs to incorporate crisis management and communications responses, including:

- Strategic plans for communications – protocols, contacts
- Shared incident management and incident response plans
- Shared governance and decision making

9.5 Crisis Response

The Open Banking Implementation Entity is only able the revoke entities from the Directory once that entity has been revoked from the relevant regulatory register by its competent authority. To respond to fraudulent activity in extreme circumstances, it may be considered useful for the Open Banking Implementation Entity to take be able to take central action to limit damage on the OB ecosystem. For example, immediate suspension of a service or Participant where clear trigger points identify a clear and present danger.

This cannot be implemented without agreement from the FCA, legal/regulatory and other experts that it is possible (or desirable) to add functionality to suspend a Participant when there is robust evidence that fraudulent activity is taking place across the ecosystem. The scope of the Open Banking Implementation Entity does not allow this action to be taken; the Open Banking Implementation Entity is required to scope and analyse potential options and gain relevant regulatory approval for any proposed process.

9.6 Sharing of intelligence relating to data breaches

The challenge for Participants and PSUs is that a data breach from one entity could then be used to perpetrate fraud at another entity, and this may not be obvious to the entity reporting the data breach. The Open Banking Implementation Entity will work with consumer groups, Participants and the Information Commissioner's Office to identify whether it would be desirable or possible for data breaches to be shared with all ASPSPs so that the ASPSPs can utilise internal fraud detection and prevention techniques to reduce the downstream impact on PSUs. This would need to balance the legal basis and PSU's privacy with the benefits to the PSU and entities involved in the ecosystem. Additionally, an appropriate legal basis will need to be identified to enable such information sharing. This and associated technical considerations will need to be fully scoped before progressing.

Glossary of Terms

For further information on the terms used within this document please refer to the Glossary on the Open Banking website at www.openbanking.org.uk

APPENDIX TWO – OPEN BANKING COUNTER FRAUD APPROACH ON A PAGE

	PREVENTION	DETECTION	RESPONSE
Open Banking Implementation Entity	• Fraud threat analysis • OB security profile • Worker vetting • Role based access to systems	• Security operations centre • Security incident and event monitoring solution • Directory enrolment process	• Revocation (after competent authority has acted)
ASPSP	• Fraud threat analysis • Directory • API risk indicators • Participant Guidelines • Counter-fraud good practice guide • Internal policies and processes	• Customer authentication & authorisation redirect • Internal policies and processes • FFA UK OB intelligence and information Sharing	• Internal policies and processes • OB dispute resolution & arbitration Model • Reimburse PSU
TPP	• Fraud threat analysis • Directory • API risk indicators • Counter-fraud good practice guide • Internal policies and processes	• Clear customer consent • Internal policies and processes • FFA UK OB intelligence and information sharing	• Internal policies and processes • OB dispute resolution & arbitration Model
PSU			• ASPSP • Information Commissioner’s Office (Data) • Financial Ombudsman Service (Financial)