OPEN BANKING

Participant Guide: counter fraud operations

A guide to implementing effective counter fraud controls

Date: January 2018
Version: v1.0
Classification: PUBLIC

Contents

1 Introduction

Open Banking enables Account Servicing Payment Service Providers (known as ASPSPs) including banks and building societies, to allow their personal and small business customers to share their account data securely with third party providers. This enables those third parties to provide customers with services related to account information such as product comparison or payment initiation using the account and product information made available to them.

This is achieved by the development, maintenance and publication of standards for Application Programming Interfaces (APIs). APIs are an established technology that uses defined methods of communication between various software components; they are used by many well-known online brands to share information for a variety of purposes.

March 2017 saw the introduction of the first Open Banking Implementation Entity standards for APIs to support access to defined elements of Open Data, as defined in the CMA Order; specifically, information on ATM and Branch locations and product information for Personal Current Accounts, Business Current Accounts (for SMEs), and SME Unsecured Lending, including Commercial Credit Cards.

As required by the CMA Order, this was followed in July 2017 by the release of further API standards for Read/Write Data that enabled Participants to publish API end points. These additional Read/Write API standards enable third party providers, with the end customer's consent, to request account information such as the transaction history of Personal and Business Current Accounts and/or initiate payments from those accounts.

Following the 2017 Budget announcement, a programme of releases to build on the core requirements of the CMA Order will be implemented throughout 2018 and into 2019.

To protect the confidentiality, integrity and availability of information and data in the Open Banking Ecosystem, all Participants should ensure that counter fraud controls are given sufficient profile in their organisation. This good practice guide is designed to provide Participants with the Open Banking Implementation Entity view on how this can be achieved.

Implementation of counter fraud controls must be in line with the Open Banking Read/Write API specifications - particularly the Open Banking Security Profile. These specifications detail the underlying information exchanges between Participants and how these are secured, but do not define the way each Participant can operate securely to meet their specific needs. This document should be read in conjunction with other Open Banking Implementation Entity 'How To' guides.

This document serves purely as a guide to counter fraud operations and does not constitute legal and regulatory advice. All Participants are responsible for their compliance with the relevant regulations applicable to their service offering and are encouraged to seek external legal advice.

2 Top Tips

- Recruit specialist counter fraud staff
- Implement a counter fraud engine to prevent and detect fraud
- Detail and maintain strong counter fraud policies and processes
- Identify, evaluate, monitor and measure fraud levels - and report at board level
- Share information and intelligence with financial services peers

3 Fraud operations

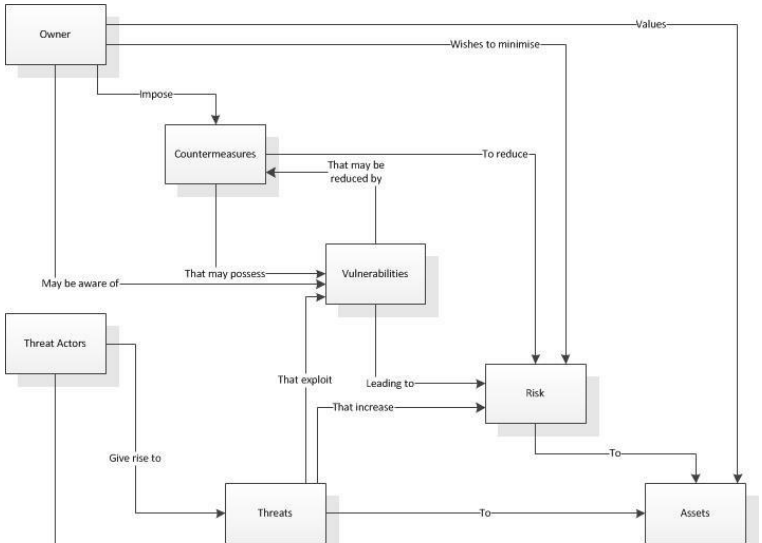
3.1 Fraud

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 is a significant threat to the UK economy and poses risk to the success of open banking transactions. In 2016, UK financial fraud losses totalled £716m and UK financial institutions prevented further losses of £1.38bn (source: Financial Fraud Action UK). Strong counter fraud prevention, detection and responses are critical to the success of open banking in the UK and the most effective way to achieve this is to implement an effective counter fraud strategy.

The minimisation of fraud risk within the Open Banking Ecosystem is considered of fundamental importance by the Open Banking Implementation Entity to ensure the protection of customers and the security of transactions. The Open Banking Implementation Entity counter fraud approach is published on the Open Banking website and details the approaches that the Open Banking Implementation Entity has considered and evaluated to mitigate fraud within the Open Banking Ecosystem.

3.2 Fraud threats

The EBA has issued guidelines on security and operational risk management which detail how Participants should implement an effective management framework. This framework requires Payment Service Providers (PSPs) to continuously monitor threats and vulnerabilities. This should include fraud threats - as they exist in all open banking transactions and could cause both financial and data losses. The threats and their impact will be specific to your organisation and having a consistent methodology for identifying and assessing threats will increase the effectiveness of your counter fraud measures. There are many published methodologies for identifying and assessing threats to your organisation - and a counter fraud specialist can help your organisation to complete a comprehensive assessment. The Open Banking Implementation Entity used the Common Criteria methodology to determine its threat assessment.



Security Concepts and Relationships (Common Criteria, 2005)

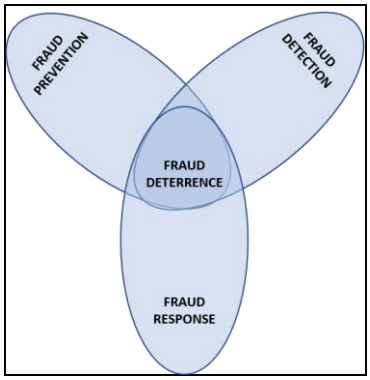
It is important that your threat analysis recognises the fraud risk which could arise from data breaches or financial transactions which could lead to financial losses - as well as any other fraud risks specific to any services you provide. The assessment should include obligations, mitigations and consequences applicable to the identified fraud risk. It can be helpful to detail fraud threats as part of your overall risk management framework, using a standard template such as the diagram below (adapted to meet your organisation's specific requirements).

Risk Ref	Threat actor	Threat category	Threat scenario	Threat vector	Outcome	Impact	Probability	Risk rating	Mitigations

ISO31000:2009 risk management standards provide a risk management framework and can be used alongside IEC31010:2009 to identify techniques and processes for identifying and assessing risks to manage them effectively.

3.3 Counter Fraud strategy

Once you have a clear understanding of your likely fraud threats, it is possible to develop a counter fraud strategy to reduce and mitigate these to acceptable risk levels. All strategies should start with clear objectives and success measures that are in line with the agreed risk appetite of your organisation.



The body of the counter fraud strategy should focus on three areas:

Fraud Prevention - including code of conduct, policies and controls, awareness training, risk assessment and management plans

Fraud Detection - including fraud detection tools, fraud reporting processes

Fraud Response - including investigation processes, data, management information and reporting, legal action, dispute resolution

The strategy should also detail other controls and policies that link to the counter fraud strategy - such as ISO27001 information security controls, internal audit function and the enterprise risk management function.

3.4 Counter fraud engine

A dedicated counter fraud engine is an effective way of automating counter fraud measures. A counter fraud engine can use multiple techniques to prevent and detect fraud and uses data and analytics to reduce fraud in payment and data transactions. Machine learning is applied to generate business rules and use cases that can quickly adapt to changing circumstances and patterns of use. Sophisticated analytics can profile users across multiple channels and identify abnormal behaviour patterns. This can be integrated with other tools to enable you to undertake detailed fraud forensic investigation and analysis - protecting your business and your customers.

3.5 Monitoring and reporting

Open Banking Participants will be obliged to monitor and report fraud levels under Article 96(6) of PSD2. The European Banking Authority (EBA) has consulted on the PSD2 fraud reporting guidelines that all Participants should incorporate into their management information and reporting processes. Fraud should be classified (commonly this is into known, suspected, attempted and prevented) and reported regularly at executive level within your organisation. In the case of open banking transactions, it is important that this incorporates both payment and data fraud. It is only through regular monitoring and reporting that the effectiveness of counter fraud actions can be measured. In the UK, FFA UK acts as the central repository for financial transaction fraud. Participants are strongly encouraged to join FFA UK and benefit from a shared understanding of fraud levels and methods to improve internal counter fraud activity.

3.6 Information and intelligence sharing

Participants are strongly encouraged to join FFA UK to work collaboratively across the financial services industry to tackle financial fraud. FFA UK is part of UK Finance and is responsible for leading action against fraud in the UK payments industry. They provide a collaborative forum for members to work together on non-competitive issues to combat fraud. In addition to working with the payments industry, FFA UK liaises with UK crime agencies to reduce and resolve financial fraud.

Data breaches should be reported to the Information Commissioner's Office. It would be good practice to also notify other Participants so that they can monitor PSU accounts for fraudulent activity and protect their Payment Service Users (PSUs) from harm. The obligations for managing personal data and reporting breaches are changing – see the Information Commissioner's Office for more details.

4 Where to go for more information

4.1 Fraud threat analysis techniques

OWASP Threat risk modelling

Common Criteria

EBA guidelines on security and operational risk management:

4.2 Fraud measurement and reporting

EBA fraud reporting requirements

4.3 Fraud intelligence and information sharing, good practice & advice

Action Fraud

FFA UK

CIFAS

Get Safe Online

Information Commissioner's Office

5 Definition of Terms

Counter Fraud Engine: A technology solution (usually provided by a third party) that can apply analytics, big data and behavioural analytics to prevent and detect fraud within transactions

Fraud: 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”

Threat vector: How a threat or vulnerability is exploited e.g. cyber-attack, browser overlay

Threat surface: The way in which your organisation is vulnerable e.g. website, databases of customer credentials

Threat actor: The person (or group) exploiting a vulnerability e.g. internal staff member, state actor

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