OPEN BANKING

SECURITY & COUNTER-FRAUD GOOD PRACTICE GUIDANCE

June 2021

1 INTRODUCTION

Security is at the heart of open banking and essential to foster continued customer trust in the safety and resilience of the open banking ecosystem.

"This security & counter-fraud good practice guidance is intended to support participant organisations in developing and maturing robust controls to safeguard them, their customers and the broader ecosystem from relevant threats."

Likewise, it's vital that participants have solid understanding of counter-fraud threats and implement appropriate controls to fight against fraud. This Security & Counter-Fraud good practice guidance is intended to support participant organisations in developing and maturing robust controls to safeguard them, their customers and the broader ecosystem from relevant threats. It's been developed in collaboration with open banking participants, industry bodies such as Cifas, and in response to feedback and insights shared through the A12 Customer Trust Consultation conducted in Q4 2020.

The guidance is designed to support a broad range of open banking participants, including TPPs and ASPSPs of varying size, maturity, risk profile and available resources. This should be taken into consideration when assessing the applicability of the guidance in developing appropriate and proportionate risk-based policies, systems, and controls for your organisation.

To further support participants with their security and counter-fraud posture and to promote a collaborative approach in response to evolving threats, OBIE invites participants to join the Open Banking Security & Fraud Working Group (SFWG). This has been established to foster cross-ecosystem collaboration, raise visibility of emerging threats, and ensure visibility of roadmap deliveries and maturing of APIs, security profiles and relevant OBIE services. To join the SFWG, please email counterfraudenquiries@openbanking.org.uk.

To complement this guidance, OBIE has also developed a Counter-Fraud Maturity Self-Assessment tool that enables participants assess the maturity of their counter-fraud control environment and identify potential areas for improvement. The tool has been collaboratively developed by the OBIE Security & Fraud Working Group, Accenture, Cifas, the University of Portsmouth Centre for Counter Fraud Studies and the Cabinet Office Fraud, Error and Debt Team. It is available free-of-charge for participants enrolled in the OBIE Directory and enables respondents gain insight into their ability to prevent and respond to insider fraud, payment fraud and other relevant fraud challenges facing financial services organisations. To access the tool please contact:

counterfraudenquiries@openbanking.org.uk.

For participants looking to formally evidence the robustness of their counter-fraud control environment, OBIE has partnered with IASME to create a Counter-Fraud Fundamentals certification scheme.[1] This certification aims to further education about and foster implementation of counter-fraud controls, as well as increasing customer confidence and trust by demonstrating participants' commitment to good practice and continued improvement.

[1] https://iasme.co.uk/counter-fraud-fundamentals/

SECURITY & COUNTER-FRAUD GUIDANCE

Effective risk management and robust security and counter-fraud controls are essential to the effective operation and resilience of the open banking ecosystem. The consequences of compromises are significant, including:

- Customer harm, including fraud or data compromise.
- Loss of customer trust and reduced take-up of open banking products and services.
- Regulatory fines or enforcement actions as a result of data breaches. Under the EU General Data Protection Regulation 2018 (GDPR), penalties for breaches of data protection could expose you to a maximum of a 4% annual worldwide turnover or €20m, whichever is greater.
- National Competent Authority (NCA) revocation of participants' regulatory status.
- Loss of revenue.
- Reputational damage.

To protect the confidentiality, integrity, and availability of the open banking ecosystem, safeguard customer data and meet regulatory obligations, including PSD2 and GDPR, it is essential that you give sufficient attention and focus to security within your organisation. Security should be at the heart of open banking products and services, with robust controls in place throughout product development, deployment and production run to ensure risks are appropriately mitigated. Embedding appropriate security controls can also support operational efficiencies: research suggests early detection and resolution of security defects can cost up to six times less than those identified in production[1].

These guidelines are intended to support you in embedding robust security controls across your organisation. Implementation of security controls should align with Open Banking Read/Write API specifications, and the OIDF Financial Grade API Profile (FAPI Profile), which outline the underlying information exchanges between ecosystem participants and how these exchanges are secured. These guidelines should also be read in conjunction with the OBIE Security Profile.

These good practice guidelines are updated regularly - including following material changes to industry standards and to the threat landscape - and are maintained in line with OBIE governance processes.

Please consult relevant regulatory documentation and guidelines, industry standards, threat intelligence and online resources for the very latest security guidance and regulatory requirements[2].

The appearance of hyperlinks or references do not constitute endorsement by OBIE of any external website, commercial company, information, products or services.

[1] https://www.synopsys.com/blogs/software-security/cost-to-fix-bugs-during-each-sdlc-phase/

[2] Relevant regulations include the FCA's Payment Services and Electronic Money approach document; EBA's Guidelines on Security Risk Management for payment service providers; GDPR security requirements etc.

SECURITY FRAMEWORKS

"It is important to select the security framework that provides the best fit for your organisation."

A range of industry security frameworks can be implemented to structure your security control environment, from foundational capabilities captured in the **UK Government's "10 Steps to Cyber Security[1]"**and **"Cyber Essentials"/"Cyber Essentials Plus[2]"** schemes, to comprehensive control frameworks such as ISO27001/2[3] and the NIST Cybersecurity Framework[4], which has an associated Financial Services profile[5] that may be useful for ecosystem participants.

For ease of reference, these guidelines are structured around the five functions of the NIST Cybersecurity Framework, which provides a common language to promote a shared understanding of security risks.

It is important to select the security framework that provides the best fit for your organisation and interpret this guidance within your own operational context, to ensure you have a fit-for-purpose control framework that adequately addresses risks in line with your organisational risk appetite.

[1] https://www.ncsc.gov.uk/collection/10-steps
[2] https://www.ncsc.gov.uk/cyberessentials/overview
[3] https://www.iso.org/isoiec-27001-information-security.html
[4] https://www.nist.gov/cyberframework
[5] https://fsscc.org/Financial-Sector-Cybersecurity-Profile

[6] Relevant regulations include the FCA's Payment Services and Electronic Money approach document; EBA's Guidelines on Security Risk Management for payment service providers; GDPR security requirements ect

IDENTIFY:

DEVELOP THE ORGANISATIONAL UNDERSTANDING TO MANAGE SECURITY RISK TO SYSTEMS, ASSETS, DATA, AND CAPABILITIES

This section helps you focus on baselining and gathering information to support your approach to embedding security - from resource allocation to understanding business context and related security risks as they relate to your organisation's business objectives.

Asset Management

Ensure physical assets (devices and systems), software, external systems, and roles and responsibilities relating to security are documented, inventoried and managed.

Business Environment

Ensure your organisation's role in the open banking ecosystem and supply chains is understood, documented and risk assessed.

Assess and document resilience requirements to support the delivery of critical services your organisation is providing.

Governance

Develop, maintain and implement an Information Security Policy, Security Strategy and associated procedures. Ensure you have allocated adequate resources, processes, technology, people and budget and that you have defined senior accountabilities and ownership for security.

Understand the relevant legal and regulatory requirements that apply to your organisation. Ensure compliance with these requirements is monitored and maintained.

Ensure security controls are regularly subject to independent testing conducted by specialist resource and results have appropriate oversight and visibility by senior management.

Risk Assessment

Ensure vulnerabilities that could impact your organisation's assets are identified and documented and appropriate mitigating controls are defined.

Maintain awareness of the evolving threat landscape by conducting regular threat assessments and monitoring threat intelligence. OBIE's Cyber and Fraud Information Sharing Exchange is a platform to facilitate sharing of threat intelligence across the ecosystem. The Security and Fraud Working Group also fosters cross-ecosystem collaboration on related topics and raises visibility of emerging threats. You are encouraged to join this group for the opportunity to collaborate with industry peers and are invited to submit suggestions for topics you would like to explore collectively. You can also leverage many of the free Open Source Intelligence sources and tools available, for example:

- SANS list of "must have" resources.[1]
- NCSC's Cyber Security Information Sharing Partnership[2] (CiSP)
- Team Cymru's Dragon News Bytes.[3]

Leveraging threat information and prioritising investment into highest risk areas will enable you to maximise value from security investments.

[1] https://www.sans.org/blog/-must-have-free-re-sources-for-open-source-intelligence-osint-/

[2] https://www.ncsc.gov.uk/section/keep-up-to-date/cisp

[3] https://team-cymru.com/community-services/dnb/

Risk Management Strategy

Ensure security risks are articulated and captured in your organisation's enterprise risk management framework. Security risks should be continually managed, with a nominated board member accountable for overall oversight.

Ensure you consider risks specific to the nature of the open banking services you provide, as well as potential risks to your customers.

Supply Chain Risk Management

Ensure security is considered during supplier procurement processes and that clear security obligations are included in vendor contracts.

Understand the risks posed by your supply chain, considering risk factors such as which suppliers have access to your systems, process personal data on your behalf or provide services that are components of your critical business processes.

Conduct due diligence and regular assurance of your supply chain, to ensure supplier security risks are managed appropriately – third parties are consistently targeted as vectors for cyber-attack.

PROTECT:

DEVELOP AND IMPLEMENT THE APPROPRIATE SAFEGUARDS TO ENSURE DELIVERY OF CRITICAL INFRASTRUCTURE SERVICES

This section helps you identify controls that your organisation can embed to protect data and ensure the delivery of critical services. The goal is to reduce the impact of a potential security event through implementing proactive defences that can support the ongoing achievement of business objectives.

Identity Management and Access Control

- Ensure robust access controls are in place to manage identities and credentials for authorised devices and users. Implement role-based access controls that apply the principle of least privilege and separation of duties, supported by robust Joiners/ Movers/Leavers processes.
- Periodically recertify access permissions at risk-based intervals aligned with the sensitivity and criticality of systems.
- Apply Multi-Factor Authentication wherever feasible to do so.
- Ensure additional controls are in place to manage and monitor remote access and privileged access. Implement secure break-glass processes to manage production access in adverse conditions, such as during a security incident.
- Ensure strong, unique passwords are in use - you may want to consider utilising a secure password vault – supported with colleague education and awareness.
- Your organisation's premises should have appropriate physical controls in place to manage and log access to buildings and sensitive locations.

Awareness and Training

- Develop a strong security education and awareness culture, supported by appropriate staff training and development. Training should cover evolving security risks, particularly phishing and social engineering, acceptable use of systems and data, information classification and handling, data management processes etc. Induction training should be provided to new joiners, with regular refresher training and awareness updates to communicate evolving threats that could implicate the organisation.
- Tailored training for high-risk colleagues is an effective means to ensure they understand risks specific to their role. For example, senior executives are frequently targeted in CEO impersonation attacks, while individuals in HR, Legal and Supplier Management functions can be at risk due to the nature of their day-to-day operational responsibilities.
- Additionally, it's essential that design and development teams are educated in secure software development practices and that they apply the principles of "security and privacy by design and default". They should also be trained on open banking-relevant security disciplines, such as API security, mobile app security etc. The Open Web Application Security Project (OWASP) foundation has a wide range of useful, free resources to support with secure application development education and training.
- Ensure all staff across your organisation are aware of their roles and responsibilities for security.

Data Security

- Protect data in accordance with its sensitivity and classification, while at rest and in transit, and throughout the data management lifecycle from creation to disposal. For example, consider database encryption for high-risk assets, ensure HTTPS is required for web traffic and require encryption for cloud data.
- Implement cryptographic controls to maintain the confidentiality and integrity of sensitive data using industry-standard algorithms, supported by robust key and secret management processes.
- Embed controls to prevent data leakage, such as implementation of data loss prevention tools that enforce policy rulesets to block exfiltration of sensitive data.
- Applying classification labels to data can assist with automation of data security controls such as digital rights management and encryption.
- Have a clear data retention and destruction policy aligned to relevant regulations, to ensure data is securely destroyed when no longer required. Over-retention of data increases security risks and cost overheads.

- Ensure development and test environments are fully segregated from production environments and security controls are embedded throughout the software development lifecycle. See below for additional information.
- Avoid using production data in non-production environments; wherever possible, use obfuscated, randomised or pseudonymised test data.
- Deploy Web Application Firewalls (WAFs) to keep your APIs secured against OWASP Top 10 security risks, zero-day threats, vulnerabilities and application layer attacks.
- Ensure appropriate controls are in place to secure cloud infrastructure. Please see the "Cloud Security" section below for further details.

Information Protection Processes and Procedures

- Define and maintain baseline configurations that enshrine hardened security for technical builds.
- Change default passwords, delete unnecessary service accounts and remove software that is not required.
- Define a Secure Systems Development Lifecycle (SDLC) that embeds the principles of "security and privacy by design and default" and supports appropriate security engagement throughout the design and development lifecycle. Embed appropriate change control processes, including formal processes for managing configuration changes.
- Wherever possible, look to automate security scanning and testing controls throughout the SDLC, for example:
- Static Application Security Testing (SAST), to identify vulnerabilities in application source code and ensure conformance to coding guidelines and standards.
- Dynamic Application Security Testing (DAST), to identify vulnerabilities in running web applications.
- Software Composition Analysis (SCA), to identify vulnerabilities associated with open source components.
- Container scanning, to scan running containers of live code in production for identification vulnerabilities or compliance issues.
- Implement a formal approach to managing policies, procedures and technical standards, ensuring these are reviewed regularly and kept up-to-date.
- Embed vulnerability scanning and patch management processes to ensure systems are kept up-to-date, stable and protected from threats. Unpatched vulnerabilities remain a common vector of attack: ransomware attacks such as WannaCry and NotPetya could have been avoided if systems had been patched on time.
- Ensure security is embedded in HR policies and practices. Screen all new recruits, embed insider risk controls to mitigate malicious or accidental incidents from internal staff. While a "no blame" culture improves transparency and early reporting of security incidents, incorporating disciplinary consequences can be a helpful deterrent of repeated poor security behaviour.

Maintenance

Implement processes to ensure your organisational assets can be maintained and repaired in a timely fashion, with approved and controlled tools and logging of related activities.

3rd party connections should be monitored, with access restricted according to defined processes.

Protective Technology

Embed layered "defence in depth" protective controls where relevant: consider including system segregation to segment high-risk areas of your estate; next-generation firewalls and DDoS prevention to protect against malicious traffic; application whitelisting to block execution of unauthorised code; web and email gateways to prevent malware ingress and intrusion protection to avoid unauthorised network access. Blocking of uncategorised websites is a useful mechanism to prevent any malware that manages to infiltrate your network from beaconing out.

Ensure event and audit logs are captured and consolidated in a Security Incident & Event Management (SIEM) solution for ongoing alerting and monitoring.

Implement controls to block removable media wherever feasible. Harden end-points, leverage Mobile Device Management Software on mobile devices and implement Bring Your Own Device policies and controls.

DETECT:

DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO IDENTIFY THE OCCURRENCE OF A CYBERSECURITY EVENT

Detect controls are designed to enable you rapidly discover security events within your organisation.

Anomalies and Events

Build a baseline of view of expected network operations and expected data flows for users and systems, so you can swiftly recognise anomalous behaviour that does not fit expected patterns.

Ensure data collected in the SIEM is correlated and analysed to understand attack targets and methods, determine impacts and establish escalation thresholds.

Security and Continuous Monitoring

Implement policies and procedures to continuously monitor for and detect anomalous events, to enable you to respond to these events appropriately.

A Security Operations Centre can help you to monitor and respond to security alerts and events, and defend your enterprise systems. You may elect to outsource your SOC, run in-house or adopt a hybrid model, depending on your requirements and capabilities. Many SOC providers have offerings tailored to align with your organisation's risk profile. While you may consider that a full SOC-type service is not required, you should nonetheless ensure appropriate mechanisms and controls are in place to detect and respond to suspicious behaviour, potential security events and possible fraud, as required by FCA and EBA guidelines.

Combine heuristic and signature-based anti-malware detection capabilities to identify potential malware outbreaks within your organisation.

Consider additional detective controls such as rogue device detection, intrusion detection and user behaviour analysis to identify anomalous behaviour that could indicate security events.

Carry out regular vulnerability scans across your estate. Frequency of scanning should align to the criticality of systems or assets, or align with threat intelligence.

Engage experienced external penetration testing services to assess applications and infrastructure for weaknesses on risk-based intervals and following material change.

Conduct red team testing to get a holistic view of how an attacker might exploit vulnerabilities or conduct social engineering to compromise your environment. In red team tests, the testing team mimic the actions of an adversary to test how well your organisation would fare in the face of a real attack. The team can use any technique that would be available to real attackers, including technology-based attacks, social engineering attacks such as impersonation or phishing, or potential physical compromise.

Monitor your organisations digital footprint to detect misuse of your brand and identify fake websites or apps impersonating your organisation. App stores are seeing an increase in fake apps impersonating legitimate financial services providers in order to phish authentication credentials from users.

Detection Processes

Develop playbooks to accelerate your SOC's response to common incident types. Tools can be utilised to automate certain types of playbook response; for instance, an automated workflow to automatically investigate a suspicious IP address and run information from threat intelligence sources, and more. This saves time and resources and provides the SOC team with actionable intelligence quickly.

Utilise threat modelling frameworks such as the MITRE ATT&CK framework to define and mature use cases for logging, monitoring and detection of anomalous behaviour.

Implement detective processes to identify shadow IT or unauthorised cloud services.

Consider actively monitoring your third-party service providers for unusual behaviour, such as unexpected traffic or log-ins.

Social media monitoring can detect security risks such as malicious links on your brand's accounts or impersonation of senior executives.

Test your detective processes to ensure these are operating effectively. Table-top exercises can help validate processes, while blue team testing can be used to validate defensive capabilities. The term "blue team testing" refers to defensive exercising to detect penetration attempts and prevent exploitation. "Purple team testing" involves both red and blue teams working together to maximise learnings and collaboratively learn about defensive controls and offensive attack methods.

RESPOND:

DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO TAKE ACTION REGARDING A DETECTED CYBERSECURITY EVENT

Respond controls support your organisation's ability to mitigate the impact of a cybersecurity incident.

Response Planning

Be prepared: define, document and test incident response plans and crisis management processes, including escalation paths, communications and stakeholder engagement. Desktop simulations and playbook reviews can be combined with technical testing and war-room exercises. Include critical third parties and relevant external stakeholders where relevant. Coverage should include consideration of how to respond to destructive attacks such as ransomware, which are becoming increasingly common.

Communications

Ensure you have clearly defined roles, playbooks and plans to map out the who, what, when, and how of notifying and engaging with internal and external stakeholders on security incidents.

External communications should be mobilised as soon as possible after you have clarified the scope and impact of the security incident and communications should focus on using concise and clear language Consider including a social media strategy in your communications plan: social media feeds can provide consistent information to a diverse range of stakeholders, including employees, customers, press and media, as well as providing insights into external impacts and sentiment.

Analysis

Ensure you have technical capabilities to investigate and analyse incidents and vulnerabilities, including forensics and malware analysis as required. This may be best achieved through engaging external specialists, building capabilities in-house or adopting a hybrid approach.

Be aware that incident data may be required as evidence for law enforcement. Consider aligning analysis procedures with best practice for processing of digital evidence – for example, guidance published by the Association of Chief Police Officers.[1]

Mitigation

Ensure incident response plans include measures to contain and mitigate security incidents and address identified vulnerabilities.

Improvements

Build lessons learned into incident management approaches and post-incident review processes. Leverage industry collaboration forums such as the OBIE Security & Fraud Working Group to learn lessons from peer ecosystem participants. The ICO has also published a helpful article on learning from lessons of others[2]; while this is a number of years old, much of the content remains relevant for open banking participants. Create a feedback loop to ensure security controls are enhanced to account for incidents and avoid future recurrence.

[1] https://www.digital-detective.net/acpo-good-practice-guide-for-digital-evidence/

[2] https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-on-line-services-learning-from-the-mistakes-of-others.pdf

RECOVER:

DEVELOP AND IMPLEMENT THE APPROPRIATE ACTIVITIES TO MAINTAIN PLANS FOR RESILIENCE AND TO RESTORE ANY CAPABILITIES OR SERVICES THAT WERE IMPAIRED DUE TO A CYBERSECURITY EVENT.

Critical in the aftermath of a security event, the Recover function lays the groundwork and outline requirements to maintain operational resilience.

Recovery Planning

Define, document and test business continuity and disaster recovery plans tailored to ensure operational resilience of critical business processes, as identified through business impact assessments. Ensure due consideration is paid to third parties providing essential support for critical processes.

Improvements

Ensure recovery plans incorporate lessons learned and that response strategies are updated to improve and mature organisational capabilities.

Communications

Ensure plans are in place to support communication of recovery activities to internal and external stakeholders and executive management, as appropriate.

Manage public relations to minimise reputational impacts associated with security incidents.

ADDITIONAL GUIDANCE

The following sections provide an overview of additional topics and online resources that may be helpful to consider.

Home Working

The Covid-19 Pandemic and resulting lockdown measures in 2020 introduced a sudden and unplanned growth in home working. A number of key technologies can support secure home working:

Virtual Private Networks (VPNs) allow remote users to securely access your organisation's technology resources, such as email and file services. VPNs create an encrypted network connection that authenticates the user and/or device, and encrypts data in transit between the user and your organisation's infrastructure.

Mobile Device Management (MDM) set up devices with a standard configuration. The majority of MDM solutions include tools to remotely lock access to the device, erase data stored on it or retrieve a backup of this data.

If home workers are using their own devices rather than corporate laptops, your Bring Your Own Device (BYOD) policy will be a critical requirement to underpin security. You should be comfortable that basic controls such as firewalls, secure configurations, access control, patching and anti-malware are operating effectively.

A key consideration is that working in a different environment can influence individuals' behaviour: research suggests that distractions such as childcare and home-schooling can result in risky security practices, including password reuse and allowing other members of the household to use corporate devices for activities such as schoolwork, gaming or shopping.

Staff also have to contend with learning curves to get up-to-speed with new software for VPNs and video-conference, along with increased risk of exposure to scams and risks capitalising on changes in working behaviour.

The NCSC provides guidance on organisational and people issues of secure home working.[1]

[1] https://www.ncsc.gov.uk/guidance/home-working

Cloud Security

The Cloud refers to hardware, software or infrastructure that exists and is managed in another data centre, and provides resources such as application services, data storage, data management, etc. While many open banking products and services leverage cloud services and infrastructure, it's important to consider specific cloud risks, in particular given regulators' focus on the concentration risk due to increased dependency on a small number of cloud infrastructure providers.

When managing cloud-related risks, standard security controls such as authentication, access control and encryption retain their significance; however, additional cloud-specific issues must also be considered, for example:

- Increased importance of multi-factor authentication.
- Tenant segregation, i.e. what controls are in place to separate your own cloud services and data from other clients of your cloud service provider.
- Jurisdiction(s) in which your data is stored, particularly in relation to personal data covered by GDPR.
- Business continuity implications and data back-ups.

The cloud involves different service delivery models, including IaaS (Infrastructure as a Service), PaaS (Platform as a Service), SaaS (Software as a Service) and DaaS (Desktop as a Service - thin clients/virtual PCs hosted in the Cloud).

In using these cloud services, certain elements of security are delivered by the Cloud Service Provider (CSP), while others are down to you. It is essential to understand the shared responsibility model and clarify security boundaries. You retain accountability for the security of ecosystem data and payments, and should ensure you have appropriate oversight and assurance in place to safeguard these.

For additional guidance on cloud controls and security, please refer to the following:

- ISO27017/ISO27018 standards for cloud-related elements of security controls and protection of personal data processed in cloud services.[1]
- Part 4 of the ISO 27036 standard covering Information Security for Supplier Relationships, which includes guidelines for security of cloud services.[2]
- FCA guidance for firms outsourcing to the Cloud.[3]
- The NCSC's Cloud Security Principles.[4]

Continuous Security Testing for Agile Development and DevSecOps

Continuous security testing and DevSecOps can be incorporated into both Agile and Waterfall approaches. DevSecOps focuses on integrating and automating testing processes and related security measures from the very beginning of the development cycle. Testing early and often results in better protection, quicker time to market and reduced costs. It can include security testing and vulnerability scans, as well as functionality and QA testing.

Continuous security testing integrates with the development process, to allow identification of vulnerabilities, remediation and retesting, to happen throughout the development process rather than applying costly post-development patches. Continuous security testing (including vulnerability scans) takes place at the end of each Agile 'sprint', as soon as functional code is available, and where possible should use tools and automated testing processes. This allows identified issues to be added to the backlog and prioritised for fixing in the following sprints. This method is particularly useful for applications developed in short iteration cycles and adds a pace to security improvements that traditional approaches can't match.

Being able to implement fixes near the point of creation removes the need for separate teams having to unpick stale code to apply fixes at a later date. Embedding security testers and QA testers with the development team also breaks down traditional barriers, spreading security knowledge among developer and thus, over time, increasing the quality of code.

Security by design and default, combined with early and continuous security testing ensures the integrity of a new application, product, or system through its entire lifecycle and avoids security being undermined in the rush to market. See the NCSC's guidance on automated security testing principles for further details.[5]

[1] https://www.iso.org/standard/76559.html

[2] https://www.iso.org/standard/59689.html

[3] https://www.fca.org.uk/publication/finalised-guidance/fg16-5.pdf

[4] https://www.ncsc.gov.uk/collection/cloud-security/implementing-the-cloud-security-principles

[5] https://www.ncsc.gov.uk/collection/developers-collection/principles/continually-test-your-security

UNDERSTANDING FRAUD RISKS

Open banking itself has not to-date introduced new fraud risks; in fact, open banking services can reduce the risk of fraud, as they don't require customers to share sensitive information with merchants. New payment services can also be leveraged to help detect and prevent fraud in other sectors, such as government services or financial relief schemes.

However, as the volume and value of transactions flowing through the open banking ecosystem continue to rise, it is likely to become an increasingly attractive target for fraudsters. As well as targeting the ecosystem using existing methods or techniques that have been successfully deployed elsewhere, criminals may also seek new opportunities that take advantage of customers' lack of familiarity with new and disruptive services. Criminals will also look to test ASPSPs' and TPPs' defences and probe customer journeys looking for vulnerabilities to exploit.

- A significant risk is presented at the customer registration/onboarding stage: weak onboarding practices are often the first of port of call for criminals looking to set-up accounts for their own purposes, using the names of genuine consumers.
- Fraud control weaknesses during customer journeys across both ASPSPs and TPPs will be sought out by criminals and exploited.
- Authorised Push Payment (APP) fraud also presents a significant risk, specifically for peer-to-peer Payment Initiation Service Providers (PISPs), as seen in elsewhere in financial services, where this type of fraud has led to significant losses.[1]
- Criminals also often target consumers who are less familiar with new payment technologies and services.

Despite where fraud liabilities or control failures sit, the impact to consumer confidence is likely to be similar - both ASPSPs and TPPs could be negatively impacted in terms of customer confidence and trust. It is therefore imperative that all parties across the ecosystem work together in helping to create a hostile environment for criminals and help support each other to effectively and collaboratively manage fraud risks.

Depending on the nature of services they provide, ecosystem participants face and present different types of fraud risk:

Service Type	Fraud risk
Peer-to-peer PISP (payment account service provider combined with PISP offering)	Payment transfer fraud - authorised and unauthorised: Money moved from a victim's payment account to another account via PISP initiation 1. Customer is socially engineered/tricked into authorising the payment instruction themselves. 2. Criminal gains access to the victim's payment account through account takeover or another means, e.g. remote access software, and then initiates payments.
PISP (merchant initiated), Card Based Payment Instrument Issuer (CBPII)	E-commerce fraud: Compromise of customer payment account information and multifactor authentication code to access their funds to acquire goods and/or other online services.
Account Information Service Provider (AISP)	Customer AISP service compromised by criminals to enable fraud elsewhere (e.g. online banking fraud - using the information captured to impersonate the victim)

[1] https://www.ukfinance.org.uk/uk-finance-cross-sector-cooperation-needed-tackle-rise-authorised-push-payment-fraud

FRAUD METHODS/ TECHNIQUES

Phishing: emails or websites aimed at duping consumers into sharing account/login credentials.

Spoofing: brand infringement: legitimate website or app is spoofed for the purposes of phishing; phone number and SMS/text are spoofed so that phone caller ID and text messages will appear to the victim as the legitimate organisations.

Vishing: phone calls to consumers to capture account credentials and/or to trick victims into initiating payments.

Smishing: text messages to consumers to capture account credentials and/or to trick victims into taking action.

Account compromise: consumer account is breached, information gleaned is used to help enable fraud elsewhere.

Account takeover: victim account is compromised and fully controlled by a criminal.

Malware: infection of consumer devices (PC or mobile) with malware enables full device takeover and capture of sensitive banking/ payment data.

SIM swap: criminals trick mobile telco providers into swapping a customer's mobile SIM to a mobile number controlled by the criminal, with all call and text messages redirected to them.

Remote access software: criminal gains remote access to victim's device (PC pr mobile), enables full takeover of all the device allows the criminal manipulate live banking/ payment sessions.

Call re-direction: criminals trick landline telco providers into re-directing a customer's to a landline phone number controlled by the criminal.

1st party fraud: fraud perpetrated by the consumer on their own account

3rd party fraud (unauthorised): criminal perpetrates fraud on victim's account.

Authorised Push Payment (APP) fraud (authorised): victim is socially engineered/ tricked by a criminal into authorising a payment instruction.

Fraud control weaknesses: control weaknesses in a participant organisation's payment journey are tested and exploited to enable fraud.

Data breach: customer data is compromised/ hacked, enabling criminals to use the information to enable fraud elsewhere.

Poor onboarding practices: poor customer registration enables fraudsters to impersonate genuine customers.

MITIGATION

This guidance aims to highlight some of the key controls that play a major role in helping to effectively manage fraud:

- Risk-based fraud strategy, with strong customer onboarding and evolving fraud controls aligned with the threat landscape.
- Regular intelligence and data sharing with peers and law enforcement.
- Joint initiatives and strong working relationships with peers and other relevant stakeholders.
- Regular customer fraud education and awareness.

"The OBIE has developed a number initiatives to help with counter-fraud efforts."

The OBIE has developed a number initiatives to help with these efforts, including the Security and Fraud Working Group (SFWG), the Counter-Fraud Maturity Self-Assessment tool and partnering with IASME on the industry Counter-Fraud Fundamentals certification scheme. Other measures include work around improving sharing of fraud risk indicators, exploring the implementation of Confirmation of Payee (CoP) checks and the APP CRM (Authorised Push Payment Contingent Reimbursement Model).

REGULATORY DEFINITIONS AND GUIDANCE - REFERENCE GUIDE

For more details on the scope/permissions of the different types of entity operating within the open banking ecosystem, please refer to information links below:

Familiarise yourself with the second Payment Services Directive (PSD2) – which has been implemented in the UK as the Payment Services Regulations 2017. You'll find guidance on the scope of the regulations in the FCA Handbook (PERG 15) and chapters 2, 3 and 17 of the FCA's guidance: Payment Services and Electronic Money – Our Approach.

You can also review the Open Banking Standard to understand what services and functionality these API specifications support.

COUNTER-FRAUD STRATEGY

There are three key features which define counter-fraud objectives: the fraud policy is the 'what', the strategy is the 'why' and 'when', and processes are the 'how'. These work collectively to support counter-fraud plans.

A counter-fraud strategy is a mid- to long-term document that your organisation should have in place to demonstrate the deliverables and practical objectives of your fraud policy, along with deliveries within specified timeframes. It helps bridge the gap between your organisation's policies and senior commitment, and actual deliverables through procedures in operational areas. It also helps identify areas for development and to ensure that your organisation is future-proof in the face of evolving fraud threats.

The owner of the Counter-Fraud Strategy is typically the Senior Fraud Manager or Head of Fraud; or, in smaller organisations, the manager responsible for the controls deployed to mitigate fraud. Approval of the Counter-Fraud Strategy should sit with either the Chief Risk Officer or a member of your organisation's Executive committee; it is the individual responsible for fraud risk, as opposed to controls, who should approve the strategy (either independently or as part of an executive committee).

The independent approval of a Counter-Fraud Strategy is key to ensure a top-down commitment and approach to counter-fraud and helps to implement a wider counter-fraud culture within your organisation.

Alignment with wider business objectives

Your Counter-Fraud Strategy should be independent and relevant to your business goals. It would be easy to set a policy or strategy with zero-tolerance to fraud, and for certain businesses, this may be a realistic ambition. For other organisations, fraud is unfortunately a common threat and a collateral cost of doing business. For example, it would be unrealistic for a credit card company to have a zero tolerance for fraudulent card transactions; instead, this type of risk would need to be assessed and managed with risk tolerance thresholds that allow for the business to operate in its market. Equally, an organisation may lend in a highly competitive sub-prime credit space, where some fraud risks would need to be accepted to offer a relevant service to the area of the market that they operate in.

Initial measurement and assessment

Often, the best foundation for a Counter-Fraud Strategy is for your organisation to collectively perform a full risk assessment of fraud risk, opportunities and controls. This type of assessment is particularly key for organisation looking to implement their first Counter-Fraud Strategy. This type of assessment will need contribution from relevant stakeholders who understand the different business processes, producs and services in detail. For example, the finance department can provide input on how mandate or invoice fraud could be committed; HR can explain how employee vetting processes might be circumnavigated to commit employee application fraud and building managers can input on how data or equipment could be removed from your organisation's premises.

Once risks are identified, an assessment of the impact and likelihood of each risk should be carried out, taking into account existing mitigating controls that are in place. The risk profile should be assessed considering both the inherent risk (i.e. without the benefit of any mitigating controls) and residual risk position (i.e. taking into account the effectiveness of existing controls already in place).

If the overall impact and likelihood of the fraud risk occurring is not materially reduced as a result of existing controls already in place, this should be identified as part of your strategy for improvement.

The example below highlights how certain fraud risks could be prioritised as part of your strategy:

FRAUD RISK	Inherant impact	Inherant likelihood	Inherant score	Existing control	Residual impact	Residual likelihood	Residual score
Mandate Fraud	8	4	32	Dual sign off for invoice payments - Change in bank details verified	6	2	12
Customer ID Fraud	6	8	48	ID and V checks	5	7	35

**As the residual risk score for identity fraud does not reduce significantly, it would be prudent to review existing controls or add further controls to counter this risk.*

"It is key that your organisation has a post-event feedback loop, that filters investigation and response outcomes back into revised governance and prevention activities. This is essential to keep your organisation up-to-date and keep pace with evolving threats."

This risk-based approach is commonly adopted and, while initiating this process can be a significant piece of work, ongoing monitoring and addition of new risks should require less effort.

For more mature organisations with a previous counter-fraud strategy in place, a natural step is to assess the effectiveness of this previous strategy and its intended deliveries. Additionally, a gap analysis of existing fraud policies can be helpful to identify gaps to consider for inclusion in the new strategy.

A key part to formulating a strategy is also to answer the question of why it is so important. This could be through management information (MI) analysis of previous fraud losses or losses in revenue due to fraud. It may possible to measure the operational demands of tackling fraud and identify areas of process improvement or efficiency gains.

Identifying objectives

A full initial assessment of risks, previous counter-fraud strategies and gap analysis of policies will most likely provide your organisation with several areas for development. To prioritise these, you should discuss business objectives with executive stakeholders, to identify those that may act as either dependencies or challenges to counter-fraud activities. You may have business objectives to launch a new product or change market strategy which will impact operational targets and therefore require support from your counter-fraud manager/team. The process of identifying objectives should require sign off from the executive board, to avoid conflicts with wider business interests or commitments to other stakeholders.

Counter-fraud objectives should be measurable, with ongoing tracking of performance. Agreed metrics might include base points of turnover, % revenue, £'s prevented, Full Time Employee (FTE) saved or customer feedback scores. Larger organisations are starting to focus on customer-centric strategies that commit to reducing customer interruptions for fraud controls, as opposed to taking an isolated view of prevention.

Counter-Fraud Strategy Framework

Many counter-fraud strategies will include a framework covering objectives and activities, grouped under Governance, Prevention, Detection and Investigation and Response. The below example illustrates details covered under each heading:

GOVERNANCE	PREVENTION	DETECTION	INVESTIGATION AND RESPONSE
Policies Procedures A Fraud Response Plan Executive Buy in and Support Risk and Control Frameworks Training	ID&V processes Segregation of duties Dual sign offs	Automated systems Whistle blowing Fraud reporting mechanisms Transaction / Event Monitoring Syndicated data sharing	Police Liason Fraud Prevention Agencies MI Reporting and Analytics

It is key that your organisation has a post-event feedback loop, that filters investigation and response outcomes back into revised governance and prevention activities. This is essential to keep your organisation up-to-date and keep pace with evolving threats.

Objectives and Timelines

Once objectives have been identified, delivery timeframes should be set in accordance with priorities and available resources. It is often helpful to publish timelines in your Counter-Fraud Strategy, to add a degree of reality around what is achievable and help prioritise resources and investment accordingly. Most strategies will add caveats to account for significant unforeseen events such as major frauds or events that disrupt the wider business.

Ongoing assessment and management

Your organisation's Head of Fraud/Fraud Manager should own your Counter-Fraud Strategy and should regularly reflect, review and reassess performance and effectiveness against agreed objectives. Where possible and appropriate, staff incentives or performance-based remuneration processes can be aligned with the strategy, to avoid conflicts of interest and time challenges. The strategy may need to be updated to take into account changes of personnel or underperformance against agreed objectives and timeframes. Whilst these should be acknowledged as accepted in certain circumstances, your organisation should go through the standard approval processes, to ensure objectives remain aligned and future-proofed.

COUNTER-FRAUD OPERATIONS

Counter-Fraud Operations are typically classified as the "1st line of defence" in organisational risk models, with compliance and audit acting as 2nd and 3rd lines.

1st line areas typically consist of specialists that handle referrals generated from the business or from automated systems you may have in place to prevent and detect fraud. Often, Counter-Fraud Operations will own the controls and systems referenced in your organisation's risk and control framework, to ensure these function as designed and are effective at protecting against, detecting and responding to fraud.

This operational area should own and maintain an inventory of Counter-Fraud Procedures, as well as ensuring resources are available to address investigations and triage significant or exceptional fraud events.

Counter-Fraud Operations	Counter-Fraud Strategy
Control owners	Risk Owners
Investigative Resourses	Assesses & identifies new products/services
Production of MI	Use MI to inform board and future strategies

Oversight and Governance

As control owner, Counter-Fraud Operations also needs to provide oversight and governance to ensure the continued effectiveness of controls - in the form of process, procedures and systems – to counter the risks these are designed to mitigate as articulated in the Counter-Fraud Strategy. Ongoing maintenance of these procedures is required to ensure accuracy and assure that they remain fit-for-purpose in response to evolving fraud threats. 1st line functions may also include Quality Assurance, to oversee the successful implementation of and adherence to procedures; alternatively this it assurance may sit within organisations' 2nd line models, depending on organisational structure.

Counter-Fraud Operations is also responsible for appropriate forecasting and maintenance of FTE (Full Time Employee) or contingent resourcing to support effective implementation and operation of procedures. Appropriate capacity and capabilities will ensure appropriate skilled and specialised resources are available, including contingency to handle significant fraud events.

For example, in a larger organisation that generate 5 FTE's worth of output, the

organisation would ideally have 5.5 or 6 FTE that includes investigations managers to respond to significant events such as material internal fraud or organised fraud attacks. Specialist resource can be utilised in quieter periods to conduct less urgent tasks such as lower priority work lists, process updates and fraud awareness programmes.

A regular challenge faced by Counter-Fraud Operations is achieving consistency in investigations. These can vary on a case-by-case basis and will invariably require a subjective decision to approve or deny relevant events, such as transactions or applications. This is a key differentiator between Counter-Fraud Operations versus other operational functions. It means that quality assurance is increasingly important to ensure that decision-making processes are clearly articulated and justified.

It is common for Counter-Fraud Operations to receive varying different types of fraud referrals requiring a risk-based approach to resolve. This can typically be achieved via a triage process with appropriate Service Level Agreements (SLAs) for referrals. Having a mechanism in place to identify and triage referrals presenting an immediate risk of loss or harm allows these to be prioritised over less urgent referrals and supports streamlined business operations.

A triage process works well for smaller teams with fewer referrals; for larger organisations receiving multiple referrals from different sources, the referral process needs to be designed in a way to apply priority categorisations, such as providing a mechanism to flag referrals for immediate attention, where urgent. SLAs requiring input from other business areas should be agreed by taking a balanced approach that assesses fraud prevention against core service delivery requirements.

Management Information (MI)

The importance of Counter-Fraud Operations' responsibility to produce, assess and report comprehensive and accurate MI cannot be understated. A range of MI is required and plays a pivotal role in ensuring that your strategy and risk thresholds are being maintained.

Arguably the most critical data to capture is evidence of how your organisation is performing against objectives to prevent fraud. MI should be captured according to the agreed format set out in the Counter-Fraud Strategy and agreed by your organisation's Executive Committee or Board, for example, either by way of basis points of revenue or turnover or by way of value and volume of losses. This helps your business measure performance against risk appetite statements and thresholds, direct future strategies and policies, and highlight areas for improvement, as well as validating effective operational processes and control.

Sharing anonymised peer-to-peer fraud loss MI through relevant industry bodies to support benchmarking is a well-established practice in retail financial services and enables organisations to measure how they perform against their peers in fraud prevention. Benchmarking outcomes and metrics can also provide a compelling business case to secure additional counter-fraud resources or budget, as well as complementing fraud intelligence and trend reporting.

An additional metric that can be helpful to consider is a resourcing forecasting model. Certain counter-fraud operational activities may be seasonal or driven by cyclical business demand. For example, customer activity may increase at evenings or weekends, so resources may need to be aligned accordingly. Your business may see increased seasonality changes, for example, in preparation for Black Friday events in November or leading up to Christmas. This illustrates the nature of counter-fraud activities not only as risk mitigants, but also as business-driven enablers.

In order to measure control and resource allocation effectiveness, you should assess the rate at which a fraud control or intervention generates false positives (i.e. where the nature of a potential fraud was falsely raised or generated. False positive rates should be particularly scrutinised in areas where the generating of potential fraud referrals interrupts the customer experience or services. It is essential to ensure false positive rates are as low as possible, while still ensuring controls are effective in mitigating the risks they are designed to address. This balancing act is key in ensuring effective ongoing processes and in validating that costs of maintaining controls are not disproportionate. While false positives are inevitable and cannot be fully eradicated, striking the right balance between false and true positives a key success factor that can be captured within your organisation's risk appetite.

Resources

Management of counter-fraud controls and systems is key to the success of Counter-Fraud Operations and requires input from both the operational team and broader strategy stakeholders. Both should give focus to understanding market innovations and products that deliver new ways of managing fraud risk more efficiently or in response to new threats. In addition, staff should be appropriately trained to fully understand operational processes and how to use available resources. It is also key to understand the skills required to respond to different fraud events while continuing to maintain business-as-usual functions.

"Taking a business-focused approach should help foster closer collaboration and strong working relationships across your organisation."

People

It's important that staff working in counter-fraud disciplines are considered as specialists and have appropriate training and skillsets to carry out their roles. For example, skills in investigative interviewing are critical to addressing internal fraud or insider threat-related investigations. Likewise, familiarity with the latest legislation and regulation applicable to investigative techniques, evidence handling requirements are essential skillsets, as is analytical expertise in managing large data sets. These should be factored in to recruitment, training and development of permanent staff and into vendor procurement activities if external support is required to support your organisation's counter-fraud operations.

An effective way of supporting staff development of staff is to allocate responsibilities within a training matrix that ensures sufficient cover and resilience to deal with increases in risk areas or in response to emerging threats. To ensure effective operations, on-hand resources should be sufficiently competent in dealing with typical daily events or referrals generated through business-as-usual activities. Certain tasks or referrals may require more senior or advanced management, such as handling of internal fraud referrals, whistleblowing referrals or investigating suspicious activity reports.

When considering the structure of counter-fraud operations area, it's important to be mindful of the fact that decisions must be made throughout counter-fraud triage processes and therefore considerations for escalation processes may be required. This could be in the form of confidentially referring complex matters to senior management, or by way of introducing senior officers or investigators to provide additional support and referral points.

The potentially sensitive nature of referrals and knowledge of business-critical risks and controls confers a higher degree of expectation around conduct of counter-fraud staff. This may be addressed through increased oversight and enhanced vetting when carrying out recruitment or supplier onboarding. Enhanced vetting for recruitment could include checks with fraud prevention agencies, credit reference agencies or disclosure and barring services, not only at the point of recruitment but on an ongoing basis as part of "fit and proper" checks.

Another element to consider when it comes to people management is how performance objectives are set. Risk aversion is, understandably, a natural inclination for of many counter-fraud specialists and is a strong asset when assessing key performance indicators and behaviours; however, to support business objectives, performance measures need to be well rounded, geared toward business risk tolerance and commercial opportunities, and supportive of customer service. Taking a business-focused approach should help foster closer collaboration and strong working relationships across your organisation.

FRAUD INVESTIGATIONS

"Your fraud policy should set out your organisation's commitment to handling fraud and details of how to prepare, resource and respond to fraud incidents."

Governance framework essentials for fraud Investigations

To support effective fraud response, your organisation should be prepared and have established protocols in place to start investigations in a structured and timely manner. You may be conducting investigations in-house; alternatively, you may seek external support; regardless of the approach, it's essential that you are well prepared to respond at pace, to protect your business and customers.

Investigations will often present various lines for enquiry and new evidence to be assessed; however, wherever possible, they should be initiated from the foundations of a tried and tested structure. The basis of this governance should include a fraud policy or policies, processes and other tools such as fraud risk and control registers. All of these should be captured, aligned and documented within your counter-fraud strategy and approved by the executive committee or board.

The fraud policy should set out your organisation's commitment to handling fraud and details of how to prepare, resource and respond to fraud incidents. A definition of fraud should be clear and relevant to your open banking services, as well as generic fraud typologies such as internal fraud, including bribery and corruption, and supplier fraud, including mandate fraud. Additional elements to cover in your fraud policy include:

- A definition of fraud as agreed by senior leadership.
- Key personnel responsible for managing fraud from a 1st, 2nd and 3rd line of defence model.
- Reference to processes involved in reporting and detecting fraud.
- A commitment to repatriating assets involved in fraud and identifying offenders.
- Tolerances and acceptance thresholds for fraud, including references to your risk and control framework.
- Details of how counter-fraud operations will be resourced, training and supported.
- A fraud response plan.

The Fraud Response Plan should form the basis for all investigations, ensuring these have appropriate ownership by those leading investigations. It should be approved by your senior executive accountable for fraud risk and may be shared with broader stakeholders. Many organisations find it helpful to publish their Counter-Fraud Policy to staff, setting clear expectations and standards relating to fraud. This can foster a fraud-aware culture and act as a deterrent, without divulging sensitivities around how fraud is detected and investigated.

A key element to consider is when the Fraud Response Plan should be invoked. Some financial services organisations encounter fraud as part of everyday operations, where invoking fraud response plans for commonly occurring incidents may not be be an effective use of time. In this case, it's important to establish what tolerances or thresholds should apply and capture these in the Fraud Response Plan. Other organisations may want to ensure the Response Plan is invoked in instances whereby customer data has been lost or if there is a risk of internal fraud. Response Plans may be triggered by financial loss, hitting exposure thresholds or on identification of related incidents that suggest a fraud ring may be in operation. There is no "one size fits all approach"; you should plan your response in line with your organisation's size, risk exposure, resources and organisational appetite.

Immediate actions and priorities

In the event of a fraud referral or detection of suspected fraud, the investigations process should begin by conducting an independent desktop review to establish the nature of the fraud and the resources required to investigate it. If the nature of the potential fraud meets thresholds for triggering the Fraud Response Plan, your Fraud Response Team should be mobilised as soon as possible. This team should consist of appropriate personnel from relevant business areas, as approved in the Fraud Response Plan. Typical representatives might include:

- **Fraud Operations**

Establish resources required and available to conduct the investigation.

- **Finance**

Representation from the Finance team is usually required to establish financial loss or potential exposure. In some organisations, the Finance function may also have broader responsibility for fraud.

- **HR**

Representation from HR department is often critical if the nature of the fraud suggests staff involvement. HR will be required to input on potential staff interviews, provide copies of employees' files, support with any disciplinary actions or suspensions and ensure colleagues' employee rights are supported.

- **Communications**

As well as losses, serious frauds may cause reputational damage or impact customer trust. Likewise, some frauds may reach the public domain before an investigation is complete. It's important that your Communications team can manage your organisation's response if questioned by the press or public in relation to the incident. This is key to maintain control of an incident and to ensure a streamlined approach to communications, both internally and externally as relevant.

- **IT, Security and Compliance**

It's typically helpful to have support from IT, Security and, where relevant, Compliance teams, particularly where fraud may require regulatory reporting. The fraud may also encompass incidents such as data breaches, which should be reported to your Data Protection Officer and onward to relevant regulators (e.g. the Information Commissioner's Office).

IT and Security representatives can help identify any technical controls that may have been breached, secure compromised accounts or services and identify control gaps that may have contributed to the fraud. Security may also be responsible for obtaining necessary evidence such as CCTV, computer forensics, system logs, access records etc.

- **Chief Risk Officer/Chief Executive Officer**

- Your organisation's CRO or CEO can approve investigatory costs and provide senior leadership and risk accountability. Senior executives may also need to be briefed around potential media, reputational and/or public impacts.

It's essential for the Fraud Response Team to meet as quickly as possible and ensure confidentiality about the nature of the fraud and subsequent investigation is maintained. In the initial meeting of the team, the lead investigator or Fraud Officer should present the nature of findings so far and agree immediate priorities.

This immediate timeframe is sometimes referred to as the 'Golden Hour', a time-sensitive opportunity where assets, evidence and witnesses are most likely to be identified and secured. The longer it takes to identify losses or evidence, the more likely these may be lost or deliberately destroyed by perpetrators.

During this initial meeting, several of lines of enquiry or avenues for investigation may be suggested. The Response Team should focus on time-sensitive elements first, specifically, material, assets and people (MAP).

Material

Key materials to be identified as early response priorities are resources required to investigate or to secure as evidence. Examples could include account access records, physical security records, computer forensics or CCTV records which often have a short retention period. These priority assets should be acquired, covertly where possible, with the assistance of IT and Security, and assessed for relevance.

Assets

Assets should be secured as swiftly as possible. If the fraud involves compromised accounts that have been inappropriately accessed or hijacked, these should be secured. If system vulnerabilities have been identified, these should be remediated. The next priority in respect of assets is to try and recoup any losses. If the loss involves financial transactions or bank transfers, it may be possible to contact the recipient financial organisation or bank to secure funds before these can be transferred again. Even if financial transfers occurred a few days before the fraud was uncovered, the receiving bank may have frozen the recipient account to validate the source of the funds, as part of anti-money laundering procedures.

People

The key priority from a people perspective should be to establish and identify victims. If your organisation's customers or suppliers have been identified as victims of the fraud, they should be contacted immediately to make them aware of the fraud and reassure them that appropriate steps are in train to rectify the matter. Compliance and regulatory specialist input may be required to provide advice and guidance to ensure regulatory procedures relating to customer protection are followed.

The next priority is to identify potential suspects or witnesses; engagement with HR is key to agree an engagement approach. The Response Team should also identify people and resources required to investigate the fraud, including the appointment of a lead investigator responsible for onward coordination of the fraud response, assignment of actions and execution timelines. The lead investigator should also manage resources involved in the investigation and present progress against investigation objectives .

Objectives should be agreed by the Chief Risk Officer or CEO and may focus on achieving a criminal conviction, as well as recovering losses and supporting victims. It's important to balance materiality of losses against costs associated with civil recovery procedures; the free criminal prosecution route may be cheaper, but is typically less likely to achieve a financial return than more costly civil proceedings. The investigation will need to be conducted in a manner that secures evidence aligned with relevant legislation such as the Police and Criminal Evidence Act 1984 (PACE) and Regulation of Investigatory Powers Act 2000 (RIPA).

Costs associated with the investigation should be agreed and approved, with ongoing management sitting under the ownership of the lead investigator. A decision-making log should also be established to record all critical decisions and the rationale as to why these were made; this log may a focus for retrospective assessments in future reviews of how the investigation was conducted . An action log can capture key actions, including dates, times and action owners.

With a lead investigator assigned, actions should be allocated in line with 'MAP' priorities, with agreed timelines and future stop-check or progress meetings scheduled before the investigation begins.

Managing the investigation process

Now that foundations for investigations are in place, with supporting policies, procedures, a Fraud Response Plan and outcomes from the initial meeting of the Fraud Response Team established, the investigation can begin, focusing on immediate priorities.

The key to managing an effective investigation is clear communication and clear recording of processes followed. We have already touched upon the action and decision log; other investigatory notes and findings should be recorded in a chronological timeline. Stakeholders in the Fraud Response Team should be communicated with in accordance with the engagement approach agreed in the initial Fraud Response Team Meeting.

The Investigations process and gathering of evidence may take different forms, including interviews with suspects. If suspects are members of staff, interviews must be conducted in the presence of appropriately trained personnel and with support from HR. Any other interviews, especially with suspects outside of your organisation should be carried out by an accredited counter-fraud specialist or a member of law enforcement. Interviews should either be audio-recorded or transcribed, with recorded approval of the content by all present during the interview.

The gathering and storing of evidence is key to any onward prosecution or civil action that your organisation may seek to take, so it's important to be mindful of any associated legislation and regulation that may apply through the investigation.

Investigation Closure

Ideally, an investigation is closed once initial objectives had been achieved; however, this could take a significant amount of time, especially if a conviction has been identified as an objective. It's key that the Fraud Response Team continues to communicate and manage time and costs accordingly throughout the investigation's lifecycle.

There may come a point where all lines of enquiry and actions are closed, but objectives are still outstanding. At this point, the CEO or Chief Risk Officer should determine when the investigation can be closed, subject to any future outcomes, as part of a debrief. This should be captured in the decision log, with the lead investigator tasked with providing further updates as and when these are received. Your organisation may choose to cover the final part of the investigatory procedure as part of the Fraud Response Plan, or via an Operational Learnings framework.

Operational Learnings and Reporting

Many fraud strategies will support a linear process such as the one below:

Organisations should ensure that this strategy is matured through an evolving model, that follows up investigations with operational learnings and reporting, to strengthen counter-fraud controls, activities and processes.

Operational learnings can take the form of internal and external reporting. Internal reports to your organisations Operational Risk or Audit functions can ensure that a review of relevant Risk and Control registers is performed in light of the fraud committed. For example, the following questions might be considered:

- Was the likelihood of the fraud risk score accurate?
- Was the impact of the fraud risk score accurate?
- Do fraud risk management thresholds need to be reconsidered?
- Did controls exist for this type of fraud risk and did they perform as expected?
- What new controls could have been effective in preventing the fraud?

External reporting can take several forms, including reports to law enforcement agencies or fraud prevention agencies. Law enforcement reporting can have a double impact of prevention: enforcement action may be taken against perpetrators and reporting also serves as a message of intent and consequence for any likeminded fraudsters. Fraud prevention agency reports are beneficial to support your organisation's fraud prevention capabilities, as well as those of collaborative partners. It's rare that a successful fraud is an isolated incident, so by sharing data and intelligence, you can help reduce the likelihood of future successful attempts. You should also consider the type of communications to issue to your key stakeholders, including customers, partners and, if relevant, shareholders. A strong message outlining the approach you've taken to detecting and reporting the fraud can help ensure investigatory outcomes are factored in to your organisation's fraud prevention and detection strategies.

Establishing close working relationships with your industry peers and other relevant stakeholders can help you identify relevant fraud data to be shared at an industry level to improve detection capabilities.

Open banking participants, including ASPSPs and TPPs, are encouraged to populate existing fraud risk indicator fields within the Open Banking API Standards, to help improve fraud detection capabilities across the ecosystem, improve resilience and enhance customer confidence.

The OBIE Security and Fraud Working Group (SFWG) continues to drive initiatives to improve sharing of fraud data and MI, as well as threat intelligence and intelligence on evolving fraud modus operandi. All participants are welcome to participate in this forum to benefit from industry collaboration against fraud.

COUNTER-FRAUD SPECIALIST TRAINING

Types of Counter-Fraud Roles and Key Skills

Fraud is a significant issue for the UK from an economical, criminal and social standpoint. A broad range of financial services organisations are impacted; naturally, organisations have different structures and resources available to counter specific fraud risks that they face. Larger financial institutions and banks may have hundreds of counter-fraud staff, while smaller TPPs may not have any staff dedicated solely to fraud. It's essential for you to consider what roles will provide the best benefit for your individual organisation, in light of the services and products you provide, your organisational risk appetite, potential fraud exposure and available resources.

A number of key fraud roles are listed below with a description of the part that this role plays within fraud prevention and key skills required to be successful within it.

"It's essential for you to consider what roles will provide the best benefit for your individual organisation, in light of the services and products you provide, your organisational risk appetite, potential fraud exposure and available resources."

Fraud Investigations Officer/Manager

Most investigations roles will involve handling referrals or potential fraud events, evaluating information and deciding how best to pursue a line of enquiry. All roles in this area involve a significant degree of organisational and communication skills. Experience and knowledge in respect of legislative requirements when handling evidence is key, in addition to an understanding of civil and criminal prosecution systems.

Financial Crime Investigations Officer/Manager

While the skills and role are similar to a Fraud Investigations Officer, the wider remit of financial crime requires role holders to be familiar with wider economic crime such as bribery, money laundering and terrorist financing. The role requires strong knowledge of regulatory compliance and legislative requirements.

Fraud/Financial Crime Operations/Manager

Some organisations may encounter fraud as an unusual or exceptional event, while for others it's a frequent occurrence and a cost of business. Where fraud or counter-fraud controls require staff intervention, a fraud/financial crime operations manager often leads a team handling business referrals as part of the "first line of defence" model. Similar to any operations manager, leadership, communication and operational forecasting skills are required, but with the broad nature of investigation work, relevant experience is required to forecast operational demands effectively.

Fraud Analyst/Analytics Manager

Where organisations deploy fraud controls that generate referrals to staff, it's important that these controls are managed in a scalable way and are not disproportionate in cost and effort to manage the risks that they mitigate. This role requires analytical skills to access and assess large amounts of data and present key information to senior staff, as well as analysing fraud trends. Data manipulation via recognised programs such as SAS and SQL is a key skill for this role.

Fraud Risk Manager

Most organisations manage fraud risk as part of other operational risk processes, with nominated risk and control owners in addition to a log of fraud risks. This will often see a measurement of likelihood and impacts of fraud risks, both pre- and post-controls implementation to assess the effectiveness of them. A Fraud risk manager is sometimes employed to manage and improve an organisations control framework specifically in respect of fraud in its many forms including consumer, staff and business related fraud attacks.

Fraud Intelligence Handler/Manager

Larger organisations typically deploy an intelligence team to collate fraud intelligence from open sources, industry groups, fraud prevention agencies and through their organisations' data analysis functions, to help inform fraud prevention and detection strategies. For instance, they may recommend rule or policy changes in respect of new applications or suggest new products or services to integrate into industry good practice. Fraud intelligence teams can also provide reports to aid investigations.

For smaller organisations, fraud intelligence data can be sourced via the Open Banking Cyber and Fraud Information Exchange. This platform can be accessed by all open banking participants registered in the Directory and provides regular updates threat and fraud intelligence information. Fraud intelligence is also shared at regular intelligence sharing and collaboration sessions led by the Security & Fraud Working Group.

Fraud Strategy Manager

A fraud strategy manager typically sits as part of an organisation's second line of defence, responsible for setting and overseeing the organisation's fraud strategy. While this role does not directly handle investigations or fraud referrals, experience in what is required is key to understanding what can be reasonably expected in terms of policy commitments and operational demand. Often, the fraud strategy manager engages with wider industry to understand new tools and services on the market and establish if the organisation's controls are up-to-date in respect of new trends. The strategy provides the framework that links organisational objectives set out through fraud policies with what is actually delivered as part of operational processes.

Counter-Fraud training essentials

Essential skills for counter-fraud professionals are relevant to the industry they operate in and the services their organisation offers. You should ensure that any counter-fraud professionals that you employ or engage are familiar with open banking, services to customers and integration with the ecosystem. A key skill is the ability to recognise risk and understand how to manage it practically and strategically. Understanding how counter-fraud tools and monitoring systems are deployed is equally important, especially how these can be matured to address emerging fraud trends.

Some sort of fraud is inevitable, therefore, at a minimum, a basic understanding of legislative and regulatory responsibilities impacting your organisation is important, particularly how and where fraud reports should be made and how these can be investigated.

Investigations experience, as a minimum in respect of open sources, should be covered – a number of industry partners offer Open Source Investigations training. A basic understanding of managing a response to fraud in the form of a Fraud Response Plan is also required – depending on your organisation's fraud risk exposure, you might find it helpful to incorporate this in your internal training on policies and procedures.

A key attribute for any counter-fraud professional is the ability to train other people themselves. If your organisation has a dedicated fraud team, a degree of cross-training is required, in addition to training any new staff, either joining as external hires or from within the company. Another key attribute to consider is the ability to deliver fraud awareness training across the business. The first line of defence for most risks, including fraud, is your operational staff dealing with customers and transactions. With fraud threats ever-evolving, established fraud controls can miss things or become outdated. Often, the best fraud reports come from customer-facing staff, so delivering fraud awareness training to all staff in your organisation can provide another avenue for detecting emerging fraud types.

Advanced Counter-Fraud Training

Some elements of counter-fraud work may require specialist training, depending the nature of your business processes and frequency of investigations.

Investigative interviewing

If fraud investigations are common practice in your organisation, specialist training in interviewing may be required to ensure you can elicit necessary information in an effective, safe and legal manner that is suitable for use as evidence in prosecutions.

CCTV and surveillance

If physical fraud and theft is more prevalent in your organisation, you may need staff to be trained in appropriate use of CCTV and surveillance, in addition to other physical security controls designed to detect and investigate fraud and theft offences.

Legislation and court proceedings

If your objective is to ensure instances of fraud are reported to law enforcement and seek prosecution, an understanding of relevant legislation and court proceedings is essential. This can cover the writing of witness statements, preservation of evidence, maintaining a chain of custody and disclosure. Good working knowledge of both criminal and civil justice systems are key to ensure you can seek convictions for any instances of fraud. Legislation such as the Fraud Act 2006, Proceeds of Crime Act 2002, Theft Act 1968, Police and Criminal Evidence Act 1984 and Money Laundering Regulations 2007 are all examples that apply when seeking to prosecute.

"It's essential that your organisation recognises the role you play in preventing fraud across the open banking ecosystem, and keep your skills, knowledge, procedures, systems and controls up-to-date and aligned with fraud trends."

Document examination

Dependant on the nature of your business and the risk of documentation fraud, training and qualifications in respect of examining documents may be required. This could be related to identity documents, received as either originals or digital copies, whereby hash-based techniques can be beneficial.

Transferrable skills and aligned roles

Many different roles across various industries can fall within the definition of a Counter-Fraud Professional. Many organisations do not have dedicated Counter-Fraud Specialist staff – roles are blended to cover additional responsibilities. Certain broader, risk-based roles can provide valuable experience in your organisations efforts to combat fraud. Examples include financial crime specialists, credit or underwriting analysts, compliance or risk specialists and auditors. Experience in these areas may present transferrable skills that can be considered to support your counter-fraud objectives.

Keeping up to date

With fraud types and modus operandi continually evolving, it's essential that skills and knowledge are kept up-to-date. The innovative and disruptive products and services within the open banking ecosystem could result in the emergence of brand new fraud trends never previously before, particularly as fraudsters' techniques become ever more sophisticated. Organised crime groups often compromise of fraud professionals and career criminals who swiftly learn and adapt to market changes and new prevention techniques. For example, the adoption of two-factor authentication for banking transactions saw the emergence of SIM swap fraud in the early 2010's. Often, new fraud controls cause frauds to diversify and adapt it into something different; understanding these evolving trends is key to ensuring your organisation is at the forefront of fraud prevention. The OBIE SFWG and prevention agencies such as Cifas actively share fraud intelligence and provide mechanisms for members to collaborate rather than compete when it comes to fraud prevention. Industry trade bodies can also be a support to agree best practice against evolving fraud and financial crime prevention requirements. It's essential that your organisation recognises the role you play in preventing fraud across the open banking ecosystem, and keep your skills, knowledge, procedures, systems and controls up-to-date and aligned with fraud trends.

ONBOARDING - KNOW YOUR CUSTOMER (KYC) & CUSTOMER DUE DILIGENCE (CDD)

If your open banking products and services involve the onboarding of customers, this section provides guidance outlining KYC and CDD requirements, and the information that should typically be collected to ensure a risk-based approach is adopted. If this is not relevant to your organisation, you might still find this section helpful context.

Open banking participants should consult relevant EBA and FCA regulatory documentation and guidelines for specific requirements[4]. For further guidance around how these regulations apply to your organisation, you may find it helpful to consult with relevant industry or trade bodies.

"ID&V measures should be proportionate and relevant to services offered."

Basics of Identity &Verification (ID&V) and KYC

ID&V as a term is often used in its own right, sometimes without referencing the full meaning. ID&V stands for "identity and verification"; essentially, identifying a person and then verifying that they are whom they say they are. This stretches beyond confirming that a person exists - organisations have to be confident that it is that specific person presenting themselves as an applicant. Verification of an applicant often requires you to verifying the information presented independently from the applicant from a reliable source; it's best practice to use a range of sources to verify an identity, including electronic records from identity providers. ID&V measures should be proportionate and relevant to services offered.

The term 'KYC' stands for 'Know Your Customer' or 'Know Your Client'. It refers to the process followed to establish the identity, suitability and risk that a potential relationship presents in respect of an organisation's Anti-Money Laundering (AML) obligations. KYC is often applied both at the start of a relationship and also throughout the relationship, as part of ongoing checks and risk assessments. This process involves collecting relevant information to establish the risk of a relationship, including details of a person or company's identity, its source of funds, wealth and other risk factors such as Politically Exposed Persons (PEPs), sanctions data or adverse media indicators. Again, the extent to which information needs to be captured, documented and evidenced should be relative to the risk that the relationship and service present in respect of potential money laundering.

When it comes to relationships with businesses, charities and companies, it's common for an organisation's obligations to stretch further, to identify persons of significant control and ultimate beneficial owners of a company. Organisations often use open sources such as director information to achieve this, including Companies House records. If a company is part-owned by another company, it's essential to establish the layers of corporate information to identify all parties involved in the potential relationship.

Many of the required processes are set out in regulation and legislation and relevant organisations need to be fully cognisant of how these apply.

4. https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

https://www.fca.org.uk/firms/financial-crime/money-laundering-regulations

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

Understanding ID&V Systems

It is critical to understand not just what a system states it does in respect of ID&V, but also how it does it. Many ID&V systems will provide a clear 'pass' or 'fail', which will dictate whether alternate ID&V processes are required. It's important to understand what contributes to a high pass or fail rate, in terms of the data sources that the identity provider uses. Traditional ID providers may traces of financial information as key data sources, including bank accounts, mortgages and utilities. Others rely on alternate services like credit cards, loans, telecom contracts or mail orders facilities. When managing ID&V systems, it's typical to take a risk-based approach regarding what data sources are being used to identify an individual. Traditionally negative data sources such as bankruptcies and County Court Judgements (CCJs) may provide be positive indicators of identification and flag creditworthiness concerns. It's important to understand this level of detail in order to design an efficient and suitable identification process that balances risks, controls and customer experience.

The same goes for verification; different data sources can be leveraged, including knowledge -based authentication, open source information including social media, copy documents and biometric data.

When assessing the suitability of a system for these purposes, you should understand what kinds of Management Information (MI) can be obtained from the system to monitor performance. Small tweaks to data sources and configurations can provide significant benefits in terms of safe pass rates and also in detecting indicators of fraud. Organisations may also need services to be configured differently when dealing with products and services presenting varying risks in respect of fraud and money laundering.

It's rare that organisations can deploy one single system to cover all business requirements in respect of onboarding; different systems may also be required for fraud and financial crime risk controls. Organisations should understand clearly what roles each of these systems perform and how they can be integrated, to avoid duplication or unnecessary service disruption.

Fraud and Financial Crime Compliance considerations

When designing systems and processes to align with regulatory guidance, it's very easy to overlook the core necessity to prevent fraud and financial crime. Ultimately, identifying and validating that a person is who they say they are may be effective to preventing identity fraud occurring; however, other controls may be required. First party frauds through misrepresentation, misuse of facilities or money laundering require additional controls during onboarding, such as checks for fraud history with fraud prevention agencies and effective KYC and CDD processes.

Equally, a typical AML risk assessment may suggest that the risk of money laundering is low for the specific product relating to the application; however it nevertheless may present a high risk of identity fraud that can potentially enable other fraud types. For instance, the financial risk and money laundering risk in supplying a credit file to an individual may be considered low; however, the copy of an individual's credit file in the wrong hands could be particularly valuable to a fraudster looking to bypass knowledge-based authentication controls with other service providers. Another example of this is SIM Swap fraud. The telecommunications sector had to bolster their fraud controls when the process for issuing replacement SIM cards to customers was abused by fraudsters to facilitate account takeover in the banking industry. Considerations need to be made of potential reputational risks that can arise if fraud controls are not sufficient robust, even if the ultimate financial risk lies with another service provider, potentially in another industry.

A risk-based approach to due diligence

Most regulatory guidance suggests organisations take a risk-based approach with respect to what information is collected from customers, taking into consideration the product being offered. The expectation is that this risk assessment is applied on an individual relationship basis, with typical relationships capturing a baseline level of information from applicants in the form of Standard or Customer Due Diligence (CDD).

CDD should reflect the level of checks and information gathered from potential customers in the typical manner of processing, and should account for the majority of relationships. Organisations should also apply measures to detect relationships of increased risk and, where these are detected, collect further information in the form of Enhanced Due Diligence (EDD).

EDD processes should be discernibly different from those covered by CDD, including collecting additional information and performing additional checks. These checks are typically carried out on an ongoing basis throughout the relationship with the customer.

There may be situations whereby a particular relationship presents a lower risk of fraud or financial crime, in which case what is often termed as Simplified Due Diligence (SDD) may be applied. SDD can see lower risk relationships onboarded more quickly by collecting less information; however, it's essential to document clearly why the relationship was considered suitable for SDD. Some organisations apply this to returning customers or for services with particular limitations such as child savings accounts.

Factors in assessing risk

KYC processes are designed to collect enough information to perform a robust risk assessment. Answers to certain questions relating product being offered should be assessed, often in a structured matrix, to determine whether the relationship is Low, Medium or High risk, in order for for SDD, CDD or EDD to be applied. At a minimum, the following as risk factors should be considered:

FACTOR	RATIONALE
Product	The product being offered needs to be assessed for its potential use for fraud or financial crime. This could include the potential for criminals to realise cash assets from the service.
Customer	Individual relationships should be assessed to establish the risks such as individuals with fraud history with fraud prevention agencies, Politically Exposed Persons, Senior Political Figures including relatives or close associates. When entering business services, firms should consider the nature of the trade or industry that the business operates in in addition to any complexity in ownership structures.
Delivery	Product delivery channels should be considered. For example, it may be determined that a face to face service presents less risk than online services.
Geography	Where the customer resides, or in the scenarios of business relationships, where they operate should be included in the risk assessment. This is in order to assess the risk of breaching sanctions or bribery and corruption risks. The Financial Action Task Force (FATF) or the Transparency International Index may be useful for this assessment.

Balancing Commercial Considerations

While your organisation's Risk department will be key stakeholders for the design of onboarding ID&V and KYC processes, in order to ensure services provided to customers support business goals and are viable and competitive, significant influence and balance is needed. Senior leadership (e.g. in the form of either a Chief Risk Officer (CRO), Money Laundering Reporting Officer (MLRO) or Nominated Officer if applicable) should have approval for where the business decides to establish its appetite, to balance offering an expedient service that is prone to risk against a service that is more cumbersome but prevents risk.

Once regulatory compliance is assured, the risk-based approach to fraud and financial crime should be documented by accepting risks captured and acknowledged by senior leadership. Many start-ups' strategies flex their approach as part of early product and service offerings. Some may launch with a very secure and risk averse product, before carefully considering partial removal or increased flexibility of controls, once forecast risks are better understood and the impact of controls on rapid growth and customer adoption can be assessed. Others may choose to launch with processes that are compliant, but with a wide degree of risk tolerance initially accepted in order to achieve early growth projections, before refining and applying controls to scale back after their product is established. Your approach will ultimately have to be compliant with legislation and regulatory guidance and should have assurance from either internal compliance expertise or external professionals.

Key specific reference points

When establishing processes for ID&V and onboarding of customers, organisations need to consider and ensure compliance with requirements.

UK businesses need to consider any applicable legislation related to their service offering, including the Financial Services Act 2012 and The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (EU's 5th Money Laundering Directive). As legislation is often difficult to interpret to a specific organisation or process, regulators such as the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) issue regulation and regulatory guidance to clarify expectations. Trade bodies also assist organisations in achieving compliance by issuing guidance and standards. A key reference point for ID&V is the Joint Money Laundering Steering Group (JMLSG), a private sector body made up of over a dozen UK trade bodies including UK Finance (UKF), The Finance and Leasing Association (FLA) and the Electric Money Association (EMA) who produce guidance to assist members to meet their obligations under UK Anti Money Laundering and Counter Terrorist Financing legislation.

OPEN BANKING

ACRONYM	TERM	DEFINITION
AISP	Account Information Service Provider	Provision of online account information services to share consolidated information on one or more payment accounts held by a payment service user with one or more payment service provider(s).
API	Application Programming Interface	A computing interface that allows two applications to talk to each other.
	API Data	Data made available to an API User or a TPP through APIs.
	API User	Any person or organisation who develops web or mobile apps which access data from an API Provider.
	API Provider	A service provider implementing an Open Data API via an API gateway.
ASPSP	Account Servicing Payment Service Provider	Provide and maintain a payment account for a payer as defined by the PSRs and, in the context of the Open Banking Ecosystem are entities that publish Read/Write APIs to permit, with customer consent, payments initiated by third party providers and/or make their customers' account transaction data available to third party providers via their API end points.
	ASPSP Brand	An ASPSP brand is any registered or unregistered trade mark or other Intellectual Property Right provided by an ASPSP.
CBPII	Card Based Payment Instrument Issuer	A Card Based Payment Instrument Issuer is a payment services provider that issues card-based payment instruments that can be used to initiate a payment transaction from a payment account held with another payment service provider.
CMA	Competition and Markets Authority	The Competition and Markets Authority (CMA) is a non-ministerial government department in the United Kingdom, responsible for strengthening business competition and preventing and reducing anti-competitive activities.
	CMA Order	The Retail Banking Market Investigation Order 2017.
	CMA Remedies	Remedies that the CMA deemed appropriate to introduce to address a number of key features of the UK Retail banking market considered to be having an adverse effect on competition. These remedies included a requirement for the UK banking industry to adopt a subset of HMT's proposals for Open Banking.
	CMA 9	The nine largest banks and building societies in Great Britain and Northern Ireland, based on the volume of personal and business current accounts. AIB Group (UK) plc trading as First Trust Bank in Northern Ireland, Bank of Ireland (UK) plc, Barclays Bank plc, HSBC Group, Lloyds Banking Group plc, Nationwide Building Society, Northern Bank Limited, trading as Danske Bank, The Royal Bank of Scotland Group plc, Santander UK plc (in Great Britain and Northern Ireland).
	Competent Authority	A Competent Authority, in the context of the Open Banking Ecosystem, is a governmental body or regulatory or supervisory authority having responsibility for the regulation or supervision of the subject matter of Participants.
	Data Standard	The data standards issued by Open Banking from time to time in compliance with the CMA Order.

OPEN BANKING

ACRONYM	TERM	DEFINITION
	Directory	The Open Banking Directory provides a "whitelist" of participants able to operate in the Open Banking Ecosystem, as required by the CMA Order. The Read/Write Directory also provides identity and access management services to provide identity information in order to participate in payment initiation and account information transactions through APIs.
	Directory Sandbox	The Open Banking Directory Sandbox is a test instance of the Directory. The Directory Sandbox may be used to support testing applications with test API endpoints and testing integration with the Open Banking Directory.
EBA RTS	European Banking Authority Regulatory Technical Standards	The European Banking Authority develops Regulatory Technical Standards which are submitted to the European Commission for endorsement. Regulatory Technical Standards are a set of detailed compliance criteria set for all parties that cover areas such as data security, legal accountability and other processes.
FCA	Financial Conduct Authority	The Financial Conduct Authority is the conduct regulator for 56,000 financial services firms and financial markets in the UK and the prudential regulator for over 18,000 of those firms.
GDPR	General Data Protection Regulation	A regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU).
	Mandatory ASPSP	Mandatory ASPSPs are entities that are required by the CMA Order to enrol with Open Banking.
OBIE	Open Banking Implementation Entity	The Open Banking Implementation Entity is the delivery organisation working with the CMA9 and other stakeholders to define and develop the required APIs, security and messaging standards that underpin Open Banking. Otherwise known as Open Banking Limited.
	Open API	An Open API or Public API is a free-to-use, publicly available application programming interface (API) that provides developers with programmatic access to a proprietary software application.
	Open Banking Ecosystem	The Open Banking Ecosystem refers to all the elements that facilitate the operation of Open Banking. This includes the API Standards, the governance, systems, processes, security and procedures used to support participants.
	Open Banking Services	The open banking services to be provided by Open Banking to Participants, including but not limited to, the provision and maintenance of the Standards and the Directory.
	Open Data	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. Open Data is data that anyone can access, use or share.
	Participant	An API Provider, API User, ASPSP, or TPP that currently participates in the Open Banking Ecosystem.
PBC	Primary Business Contact	A Primary Business Contact is an individual nominated by an entity to have access to the Directory and will be able to nominate other Directory business users. This should be a formal business point of contact and a senior member of staff responsible for systems and controls related to Open Banking.
PSD2	Revised Payment Services Directive	The Payment Services Directive 2015/2366, as amended or updated from time to time and including the associated Regulatory Technical Standards developed by the EBA and agreed by the European Commission and as implemented by the PSR and including any formal guidance issued by a Competent Authority.

OPEN BANKING

ACRONYM	TERM	DEFINITION
PISP	Payment Initiation Services Provider	A Payment Initiation Services Provider provides an online service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.
PSP	Payment Services Provider	A Payment Services Provider is an entity which carries out regulated payment services, including AISPs, PISPs, CBPIIs and ASPSPs.
PSR	Payment Services Regulations	The Payment Services Regulations 2017, the UK's implementation of PSD2, as amended or updated from time to time and including the associated Regulatory Technical Standards as developed by the EBA.
PSU	Payment Services User	A Payment Services User is a natural or legal person making use of a payment service as a payee, payer or both.
PTC	Primary Technical Contact	A Primary Technical Contact is an individual nominated by the entity to have access to the Directory and will be able to nominate other Directory technical users. This should be a main point of contact on technical configuration and a senior member of staff with responsibility for the management of the Open Banking digital identity.
	Read/Write API	Read/Write APIs 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.
	Read/Write Data	Read/Write Data includes personal current account and business current account transaction data sets made available by ASPSPs in accordance with the Read/Write Data Standard.
SCA	Strong Customer Authentication	Strong Customer Authentication as defined by EBA Regulatory Technical Standards is an authentication based on the use of two or more elements categorised as knowledge (something only the user knows [for example, a password]), possession (something only the user possesses [for example, a particular cell phone and number]) and inherence (something the user is [or has, for example, a finger print or iris pattern]) that are independent, [so] the breach of one does not compromise the others, and is designed in such a way as to protect the confidentiality of the authentication data.
SMEs	Small and Medium-sized Enterprises	Small and medium-sized enterprises by scale of business, as defined by the CMA, with a turnover <£6.5m p.a.
	Standards	The Standards are the Data Standards and Security Standards in accordance with which ASPSPs will be required to make Read/Write APIs available.
TPP	Third Party Provider	Third Party Providers are organisations or natural persons that use APIs developed to Standards to access customer's accounts, in order to provide account information services and/or to initiate payments. Third Party Providers are either/both Payment Initiation Service Providers (PISPs) and/or Account Information Service Providers (AISPs).
	Voluntary ASPSP	Voluntary ASPSPs are those entities who, although not obliged to enrol with Open Banking, have elected to do so in order to utilise the Standards to develop their own APIs, to enrol onto the Open Banking Directory, and to use the associated operational support services.