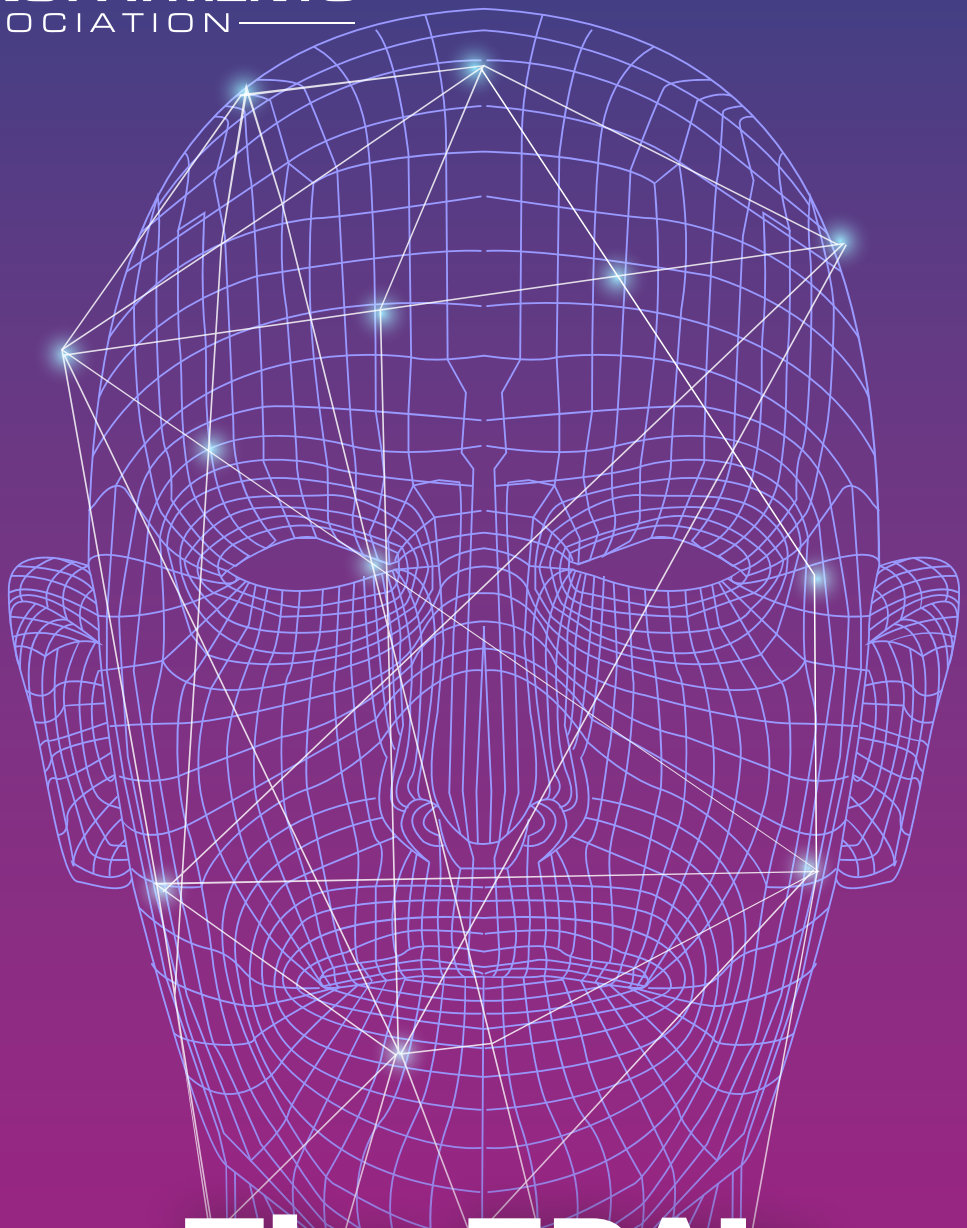
EMERGING PAYMENTS ASSOCIATION

REFINITIV™
DATA IS JUST THE BEGINNING™



The EPA's Guidebook to Digital Identification and Authentication

A guidebook to help keep you and your customers safe in the digital world

2020

Executive Summary

Identification and Authentication are important processes that help to keep you and your customers safe in the digital world. They enable you to be confident that you know who your customer is, ensuring that they are entitled to access your service and can continue to do so securely and confidently.

This is especially important in financial services and adjacent services such as gambling. In these the threat of criminal activity, including money laundering, financing terrorism and fraud, requires that robust identification and authentication are employed.

As a consequence, organisations operating in these areas are required to comply with regulatory requirements designed to tackle the threat of financial crime.

Organisations are required to take a risk-based approach, understanding both the risks present in the markets in which they operate as well as the risks to themselves specifically. Only when the risks are fully understood can the right choice of identification and authentication solutions be made.

This guide explains what identification and authentication are, presenting an overview of the technologies that can help you. It also arms you with key questions to put to suppliers when determining which solutions will meet your needs best. There are numerous suppliers in the identification and authentication space addressing different parts of the process in different ways. The body of this guide does not name specific suppliers but provides you with the information and guidance needed for you to find suitable suppliers. There are several EPA members with relevant solutions. These are listed in the appendix along with EPA ambassadors that have expertise in this area.

TABLE 1: WHITE PAPER RECOMMENDATIONS

Ref	Theme	Recommendation
1	Regulatory context	You need to understand the regulations that apply to your organisation. This should include reading, understanding and following published guidance relevant to the country in which you operate. Key regulations include Anti-Money Laundering (AML) Regulations and payments regulations, such as the 2nd European Payment Services Directive (PSD2).
2	Risk-based approach	Finding the right solution is more than just a tick box exercise. You need to understand the risks to your business, in the context of the wider risks present in the countries in which you operate. You should undertake a thorough risk assessment to determine which identification and authentication approaches best address your needs.
3	Implementation	The approach you take to implementing identification and authentication, will depend on your in-house capabilities. Some suppliers provide end-to-end solutions; others provide components that you can assemble or integrate into your systems – although that may require greater maturity and operational capability.
4	Role of technology	Identification and authentication processes can result in friction in services where you can least afford it (e.g. during onboarding). On the other hand, well implemented identification and authentication solutions can reduce friction and increase revenue. You should therefore seek to employ the technology available to improve the digital journey whilst protecting yourself and your customer from fraudulent and illegal activities.
5	How EPA can help	Several EPA members offer best of breed products and services that can help you to build the identification and authentication processes that you need.

About the EPA

The Emerging Payments Association (EPA), established in 2008, connects the payments ecosystem, encourages innovation and drives profitable business growth for payments companies. Its goals are to strengthen and expand the payments industry to the benefit of all stakeholders. It achieves this by delivering a comprehensive programme of activities for members with help from an independent Advisory Board, which addresses key issues impacting the industry.

These activities include:

- A programme of 70 events annually
- Annual Black-Tie award ceremony
- Leading industry change projects
- Lobbying activities
- Training and development
- Research, reports and white papers

The EPA has over 130 members and is growing at 30% annually. Its members come from across the payments value chain; including payments schemes, banks and issuers, merchant acquirers, PSPs, retailers, and more. These companies have come together, from across the UK and internationally, to join our association, collaborate, and speak with a unified voice.

The EPA would like to thank its dedicated project Financial Crime members for their contributions to this white paper including: Jane Jee of Kompli-Global, Jonathan Jensen of GBG, Verity Snelson and Aravind Narayan of Refinitiv, Andrew Churchill of Technology Strategy, Phillip Creed of fscom, Victoria Preece of allpay, Tim Ayling and Asaf Yacobi of Buguroo, Steve Pannifer and Margaret Ford of Consult Hyperion.

Introduction from Refinitiv

Refinitiv is privileged to sponsor the EPA Guide to Digital Identification. Our support of this guide and as benefactor to the EPA display our commitment to assisting organisations to meet their regulatory obligations to fight financial crime.

Our daily interactions can now just as easily be conducted with those across the globe as they can across the street. The need to trust those interactions can be achieved with the right technology to safe guard against fraud and money laundering. At the time of writing we are in the middle of the COVID-19 Pandemic and FATF, the global standard setter for combating money laundering, says it "encourages the fullest use of responsible digital customer onboarding and delivery of digital financial services in light of social distancing measures," Moving to digital channels introduces new opportunities for financial institutions and companies, but also criminals. Identity Theft is one of the fastest growing criminal markets, It is vitally important that organisations adopt robust digital identity verification solutions to protect themselves from fraud. In response, Refinitiv has launched 'Qual-ID', which is designed to provide a seamless consumer experience while helping to protect against fraud and money laundering. It supports fast and secure digital onboarding through a combination of Refinitiv's World-Check Risk Intelligence with Trulioo's digital identity network through one API. This guide explains how through technology and data, the most crucial factors in identifying a consumer's identity can be verified within a risk-controlled framework protecting your organisations from criminals whilst meeting your regulatory obligations.

Phil Cotter
Managing Director of the Risk business
Refinitiv

Table of Contents

Introduction

What is identification and authentication?

Regulated services often need to determine the identity of their customers and employ robust security to ensure that services are only accessed by the correct individuals or organisations.

This helps to prevent fraud and other criminal activity. The processes employed to provide these controls can be referred to as "identification" and "authentication".

Identification is the process of establishing the identity of your customer, including determining and confirming key information such as the name and address of the customer. This is a process that is typically performed when establishing a new business relationship and involves the customer providing evidence of their identity that you then verify.

Identification
"Establish Identity"

Authentication
"Use Identity"

Authentication is the process through which your customer can confirm who they are when they use your service or perform a transaction. This requires that the customer has access to authentication methods such as a secure mobile app, biometrics or passcodes. Different levels of authentication may be employed: accepting, for example, less authentication for low risk services but requiring a "step up" so that high risk services are protected by strong authentication.

Identification and authentication processes work in tandem. For example, if a customer's authentication methods are lost or compromised, it may be necessary to re-identify the customer before then provisioning new authentication methods for them.

Before designing or selecting identification and authentication solutions you should undertake a risk assessment to ensure the approach taken is proportionate to the risks faced.

Why are identification and authentication necessary?

Identification and authentication help you to ensure you know who you are dealing with, providing security mechanisms that protect both you and your customer. In financial and adjacent services, identification and authentication play a key role in preventing financial crime.

These processes fall within a broader set of requirements to "Know Your Customer" (KYC), which includes knowing who your customer is as well as ensuring your customer is legitimate and not seeking to use your service for criminal activities.

Identification technologies will help you address the following aspects of KYC:

- **Identify Customer:** identifying the specific organisation or individual concerned.
- **Verify Customer:** performing checks to confirm that you are dealing with that specific organisation or individual.

Authentication technologies help to ensure a financial account is only accessed and used by the authorised organisation and individual established during the identification process. The EU 2nd Payment Services Directive has introduced the requirement for strong customer authentication for many payment transactions.

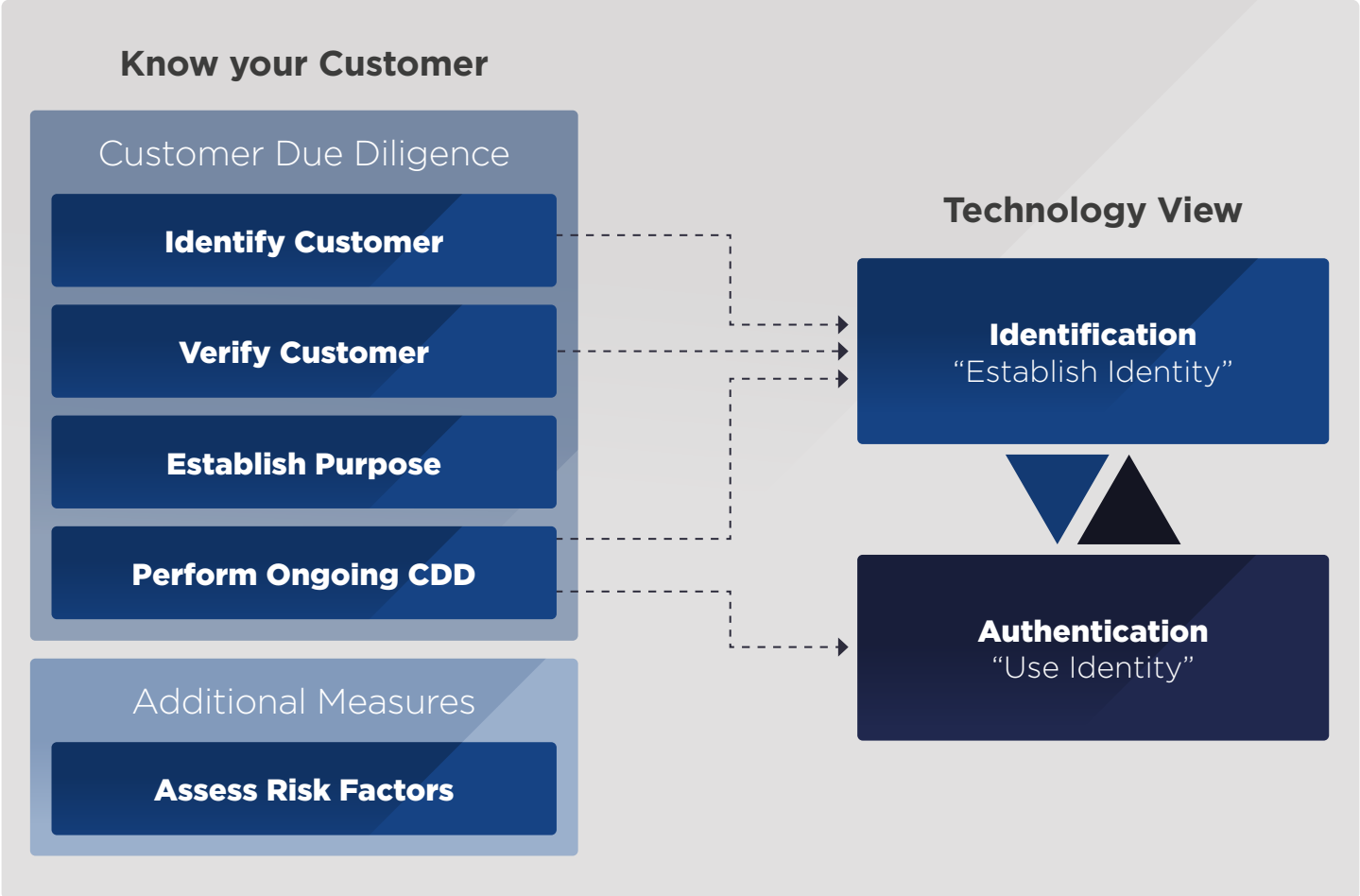
You need to meet KYC requirements before you provide the customer with a regulated service, but that is not the end of it. You will be required to perform ongoing customer diligence (CDD) throughout the lifecycle of an account. This may involve needing to identify or verify the customer again.

As well as ensuring you know the identity of your customer, you will need to perform additional measures to assess the risk associated with the customer. This could include checking external sources such as PEP and Sanctions lists, law enforcement and adverse media. This is considered further in the EPA's risk assessment guidance document.[1]

"As well as ensuring you know the identity of your customer, you will need to perform additional measures to assess the risk associated with the customer. "

Who needs to worry about identification and authentication?

Identification and authentication together help organisations prevent illegal activities including money laundering, financing of terrorism and fraud. Organisations providing financial and adjacent services[2] are required by law to ensure that they know the identity of their customers, as part of a broader set of Anti-Money Laundering (AML) rules aimed at curbing financial crime. Navigating your way through AML regulation can be complex. You should ensure that you understand the requirements for identification as they relate to your business and who you are accountable to.



1 https://www.emergingpayments.org/article/risk-assessment-guidance-document/

AML regulation requires you to take a risk-based approach rather than just ticking the boxes. You should complete your own risk assessment – looking at both your business and the risk landscape of the countries in which you operate.

The measures you employ to combat money laundering and financial crime should be designed to address the risks that exist, based on you having a good understanding of what those risks are.

Until recently authentication was not explicitly dealt with in regulation. In the UK, the Consumer Credit Act ensures that consumers are protected from fraud and that, in turn, has led to the payments industry introducing various authentication initiatives. PSD2 has gone a lot further not only requiring strong authentication to be applied to payments but defining what does and does not constitute a strong authentication.

The recently published Financial Action Task Force (FATF) guidance on Digital Identity[3] also suggests an increasing regulatory focus on authentication, alongside more traditional KYC and AML.

About this document

This guide describes the component parts of these identification and authentication processes. It highlights current solutions and technologies that you should consider using to meet your regulatory requirements and provides guidance on what to ask when working with suppliers to select a solution.

Please note this document is not intended to provide exhaustive or authoritative guidance on identification and authentication requirements. The intent is to provide organisations with awareness of the technology choices available in the market today, that may help them comply with the regulations applicable to them.

2 i.e. Designated Non-Financial Businesses and Professions (DNFBPs)

3 http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

4 https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

4 Regulation (EU) No 910/2014, https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

6 https://www.napier.ai/post/anti-money-laundering-who-regulates-me

Fighting financial crime – the context to identification requirements

Financial crime is a global problem with organised crime often transcending geographic boundaries. Consequently, international cooperation and coordination is essential in fighting financial crime and provides the context for the specific identification requirements and standards applicable in any particular country.

International

The Financial Action Task Force (FATF), an intergovernmental 'organisation', is central to this international cooperation, developing policies to combat money laundering and terrorism financing including setting standards and making recommendations for "Know Your Customer" processes. FATF monitors the implementation of its recommendations through peer review processes (referred to as "mutual evaluations") of member countries. These include evaluating the legal, regulatory and operational measures put in place by the member country, the aim being to generate the necessary political will to bring about the legislative and regulatory reform necessary to address any issues that may exist.

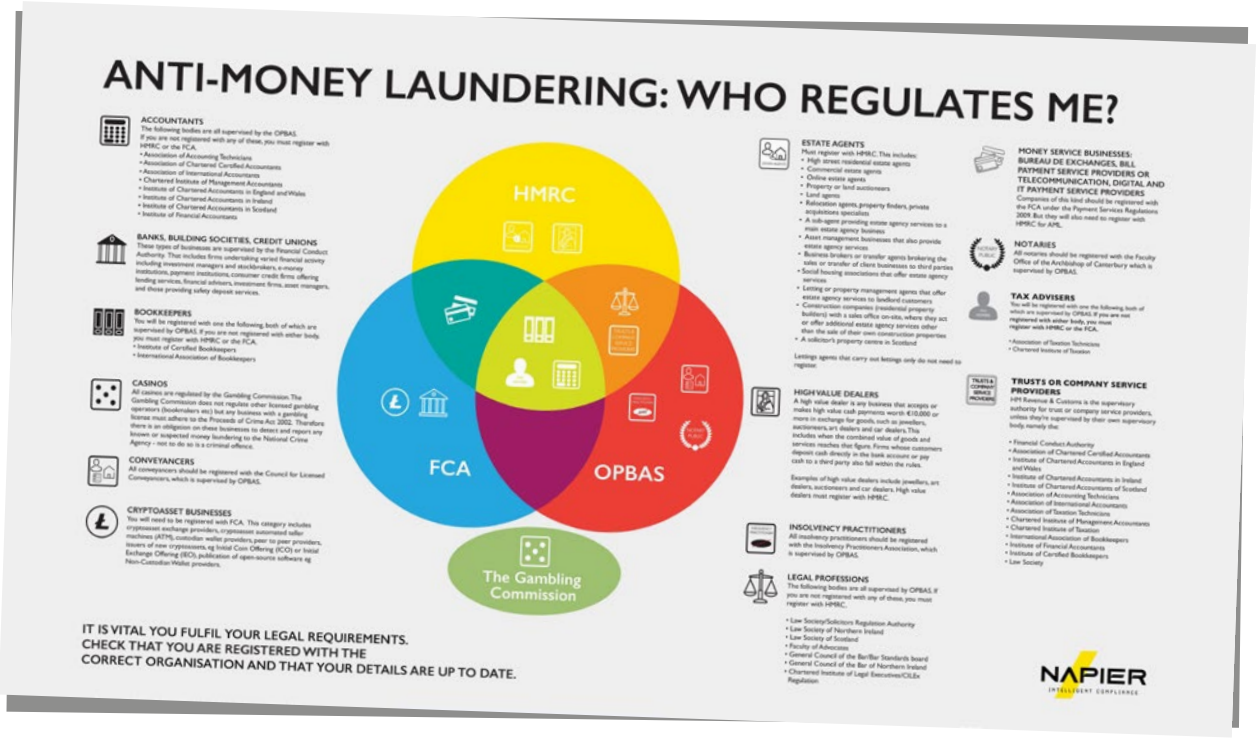
FATF has recently published guidance to help AML regulated entities determine how they may use digital identity systems for customer due diligence.[4]

Regional

In Europe, FATF works with the European Commission as well as with individual member countries.

In recent years, the European Commission has been active in driving the adoption of a series of AML directives expanding the range of services and entities in scope of AML regulation. As a result, identification checks are now required in a whole range of contexts including financial services, virtual currency exchanges, professional services (e.g. accountants, lawyers), gambling, estate agents, art dealers and more.

The AML directives state that identification must be performed "on the basis of documents, data or information obtained from a reliable and independent source" but leaves it to each individual country to deem what is appropriate.



In parallel with AML, the EU has been seeking to standardise the patchwork of government-issued electronic identity systems across Europe through the eIDAS regulation.[5] The intention is that government-issued electronic identities would provide a solution to the requirement for identification.

National

Each European member states enacts its own regulations to meet the requirements of the European AML directives and determines how those regulations are to be supervised. Consequently, the local requirements and guidance will vary from country to country, but there can also be similarities. In Austria, Germany and Spain for example, the regulators have recognised video identification technology which allows an individual to be identified via a live video chat session. This has proven very popular in those countries.

UK

In the UK, the following AML regulations apply:

- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs 2017) which came into force on 26 June 2017. These regulations implement the EU's fourth directive on Money Laundering (Directive (EU) 2015/849).

- The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (MLRs 2019) which came into force on 10 January 2020. These regulations implement the EU's fifth directive on Money Laundering (Directive (EU) 2018/843).

Napier has produced a helpful infographic on AML regulation in the UK[6] that will help you determine who regulates you. In summary in the UK there are three statutory regulators:

- FCA (Financial Conduct Authority), which supervises much of the financial services industry.

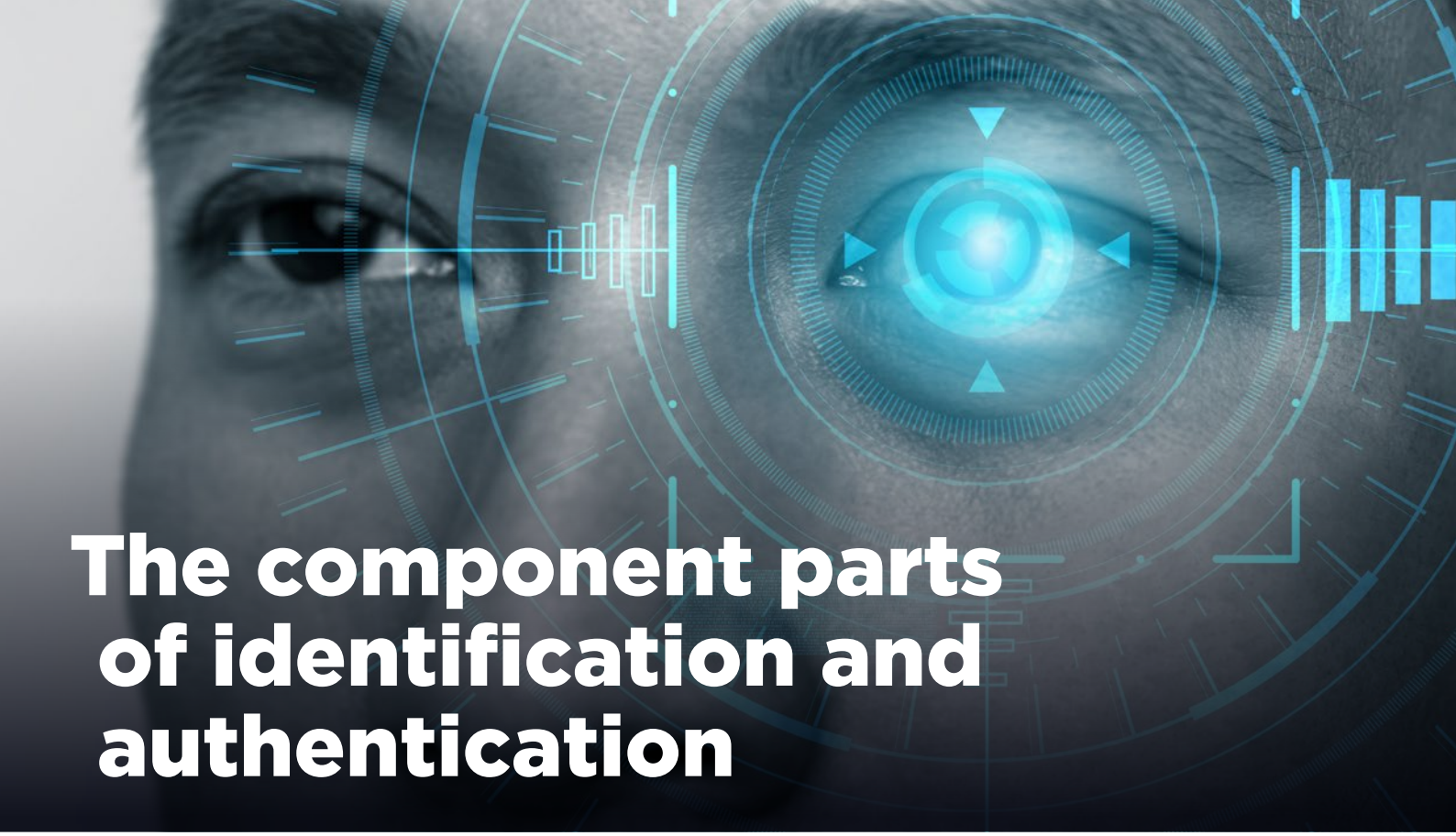
- Gambling Commission, looking after the gambling industry.

- HMRC (Her Majesty's Revenue and Customs) which supervises organisations (and sole traders) not covered by other regulators, e.g. estate agents.

There are also 22 non-statutory supervisors made up of various the professional bodies (e.g. Institute of Chartered Accountants in England and Wales) that supervise professional services.

Since 2018 these have been overseen by the Office for Professional Body Anti-Money Laundering Supervision (OPBAS), that sits within the FCA. Ultimately it is down to these supervisory bodies to determine what identification methods are appropriate or not.

In the UK, the financial services industry has established the Joint Anti Money Laundering Steering Group (JMLSG) which publishes guidance on how to meet AML requirements, including how to perform identification and the types of evidence that may be appropriate.



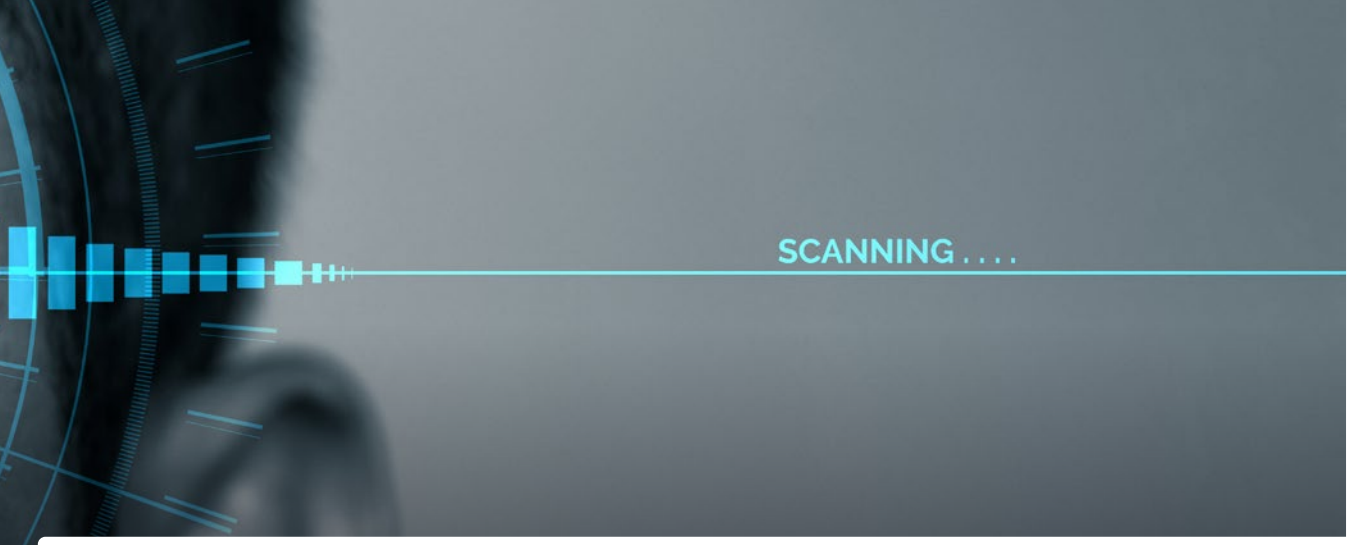
The component parts of identification and authentication

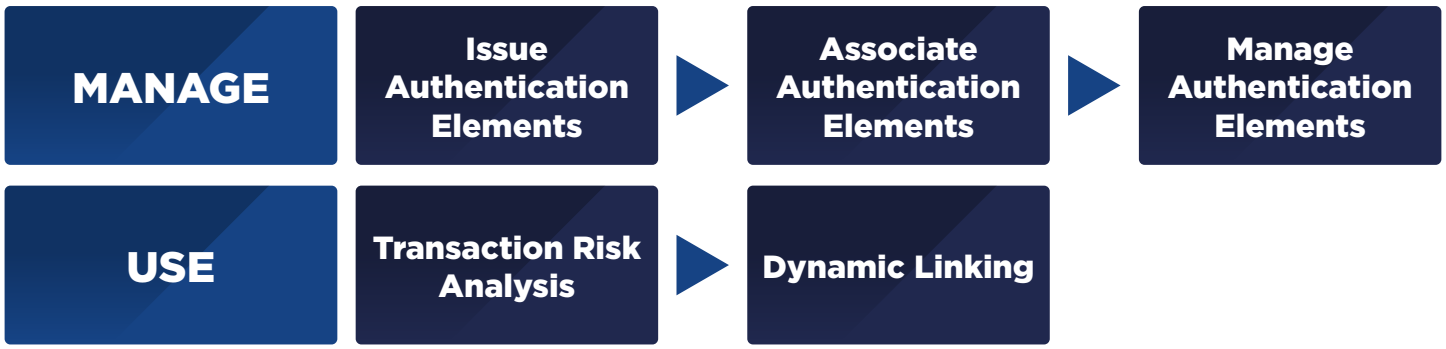
Components of identification

Identification is the process of determining who your customer is. The process applies to both business customers and retail customers (i.e. individual people). Businesses are of course made up of people and so the identification of a business also includes the identification of key people associated with the business including directors, principal officers and ultimate beneficial owners.

Identification of an organisation involves establishing and verifying the identity of the business, who owns it, its purpose and who the key individuals are. The identity of those key individuals may also need to be verified, depending on the local regulatory requirements. The process can be complex owing to the different ways in which organisations are established and registered, the complex structures of some organisations and the potential for key individuals to be located anywhere in the world.

Identification of an individual involves the collecting and verifying of evidence to confirm the person is who they claim to be. The types and combinations of evidence that can be used varies widely depending on the circumstances of the individual as well as the requirements of the jurisdiction where the





identification is being conducted.

Components of authentication

Authentication is the process of ensuring the individual using your service is entitled to do so, either acting on their own behalf (e.g. a retail customer), on behalf of another individual (e.g. using power of attorney) or on behalf of an organisation (e.g. as an officer of a business).

Authentication can be explicit requiring the individual to do something (e.g. enter a passcode, perform a biometric check). Authentication can also be implicit, analysing context, transaction and device information to detect unusual behaviour that could indicate fraud.

Usually a combination of explicit and implicit authentication is required.

"The identification and authentication market landscape is very complex with numerous suppliers providing different solutions."

Types of vendor

The identification and authentication market landscape is very complex with numerous suppliers providing different solutions.

Broadly speaking, suppliers fall into one of the following three types:

- **Curator:** provides an end-to-end identification or authentication service comprised of components that they have selected and offer as a single, integrated solution. The solution requires all clients to adopt the same standard approach.
- **Aggregator:** provides a comprehensive identification or authentication service or platform made up of components allowing the client to choose from a range of products and services offered. It is for the client to decide which components they wish to use and the aggregator to provide them. This provides greater flexibility than the curator but demands a greater level of knowledge at the specification stage.
- **Capability:** provides capabilities in a specific area such as performing a specific part of the identification process, providing access to a particular type of data or providing a specific authentication method.

Depending on your internal capabilities and particular requirements, you may wish to consider using a supplier, such as a curator or an aggregator, to provide you with a complete solution.

Alternatively, you may wish to build you own solution, selecting and integrating specific capability providers into your existing processes.

Identification of organisations

The process of understanding the structure of a corporate can be complex. When done manually, it may require multiple interactions with the corporate to gain access to the right set of documentation needed to complete the identification process.

Understanding the process

Identify and verify organisation

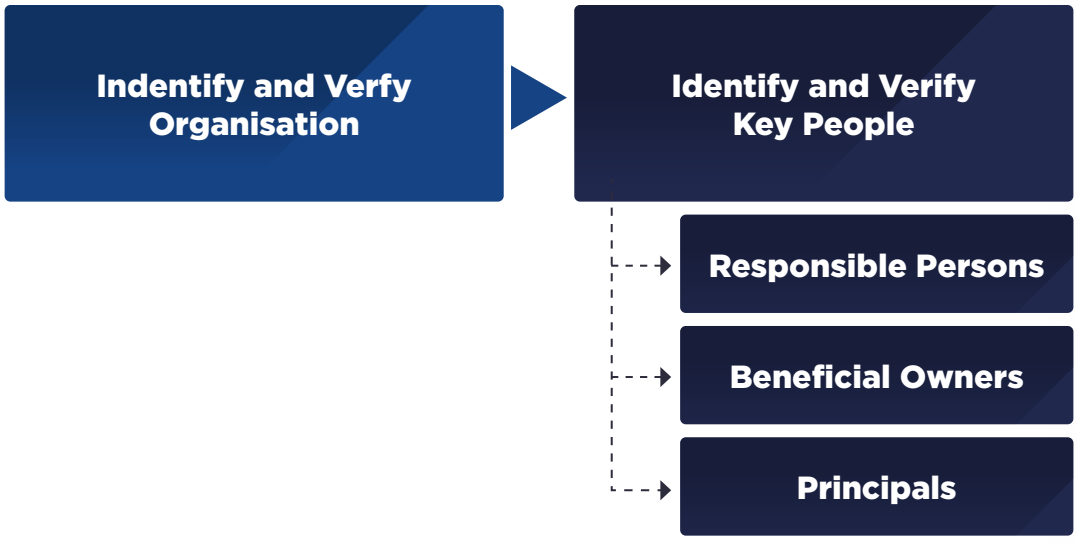
Identifying and verifying an organisation involves checks on important information, including:

1. Organisation Name.
2. Registration number.
3. Registered address.
4. Official documentation such as its constitution or articles of association.

The specific information required will vary depending on the type and complexity of the organisation.

Navigating layers of complex organisational structures is essential when investigating potential money laundering. Identifying fake companies and shell companies is a key requirement. This can be a challenging task, as such companies are naturally designed to look entirely respectable at first glance. This is an area in which high-quality checks supported by technology can be particularly useful.

If an organisation is identified as being based in, or having connections with, "high risk" countries you will need to undertake additional due diligence before entering into a business relationship with it.[7] If the organisation is identified as having links with a sanctioned country then no business relationship should be established.



7 Both the European Commission and FATF publish lists of such countries.

Example identity verification sources

- Business Directories
- National UBO Registers
- National ID Databases
- National Insurance Registries
- Driver's Licence Registries
- Passport Documents
- Bank Accounts
- Birth Index Register
- Mortality Registers
- Electoral Roll
- Postcode Address File
- Consent Databases
- Others

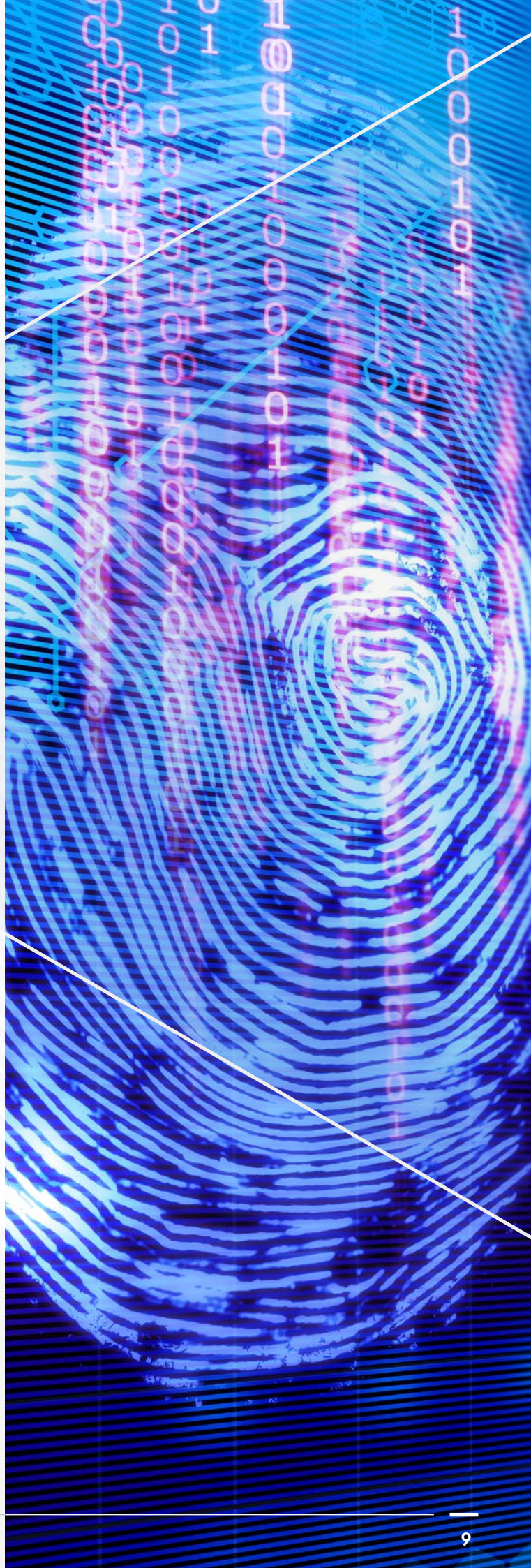
Identify and verify key people

Responsible persons
Once the structure of the organisation is established, it is necessary to map the responsible persons within the organisation. This will include understanding who the beneficial owners, directors, shareholders and persons of significant control are. These are the people who are involved in the financial and business activity of that organisation. This process can be complicated by the fact that company officers can be located in any geography. While the processes to follow may be reasonably standard , each country will vary considerably in terms of the sources available and the means of accessing them.

Ultimate beneficial owners
Ultimate beneficial owners (UBOs) are the individuals that own an organisation. Ownership may be concealed under several layers of obfuscation – hidden behind companies, trust funds or other organisations that own the actual organisation being vetted.

As with responsible persons, UBOs can be located in any geography creating challenges in identifying and verifying them. Regulations usually stipulate a threshold above which beneficial owners must verified. The threshold applied to ownership can depend on jurisdiction, the level of risk associated with the organisation as well as the organisation's own assessment of risk.

Principal
It is frequently necessary to check whether a person has the right to act on behalf of a particular organisation. This involves carrying out identification of the individual and confirming that the person identified is indeed the person designated as representing the organisation.



Choosing suppliers

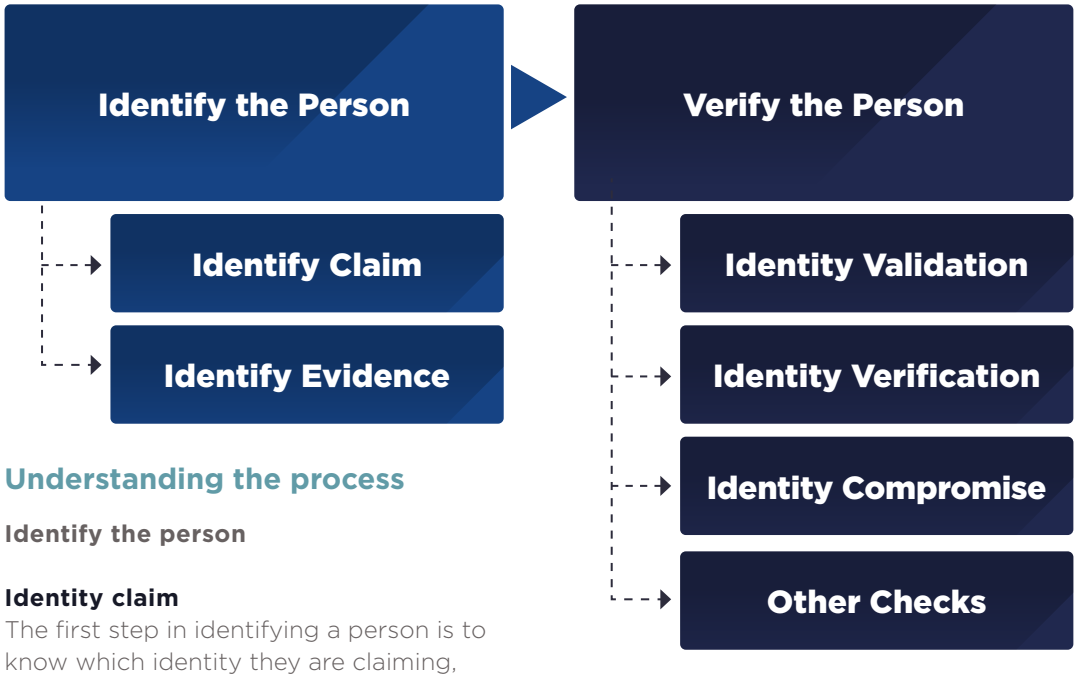
Capability	Service Type	Description
End-to-end Process		
KYB Compliance Tool	Service	"Know Your Business" (KYB) compliance tools support compliance professionals by providing a systematic approach to handling the complexities of implementing KYB.
CDD/Risk Assessment	Capability	Risk assessment is a key part of the CDD management process to ensure that the correct level of resources are allocated, in proportion to the level of risk.
Risk Rating Assessment	Capability	Apply a risk rating according to defined criteria (Low, Medium or High). This will govern the level of resources to be allocated. For example, a deposit account with minimal activity will normally require only basic levels of verification. A standard account belonging to a salaried individual with a higher number of transactions is likely to require a greater level of verification. Enhanced Due Diligence (EDD) may be required for higher risk companies and their beneficial owners.
Identify and Verify Organisation		
Customer ID Verification	Capability	Carry out checks to confirm the status of the organisation. Basic checks include confirming their legal status, registration details and operating address. Further checks may include details of the company's trading history.
Sanctions Screening	Capability	Check to identify any sanctions applicable to the client organisation. Provides access to real-time information from external authoritative sources.
Identify and Verify Key People		
Responsible Persons Identification	Capability	Identifying the individuals in authority within an organisation. These include the people who run the business (either alone or in partnership) and officers of the business, e.g. directors and company secretary. Checks include identification of the individual, as well as their role within the organisation.
UBO Identification	Capability	Identifying the ultimate beneficial owners: the individuals or organisations who own an organisation. Ownership can be direct or indirect via another organisation. Indirect ownership may involve multiple layers of complexity. There may also be issues with availability of reliable records, which varies substantially by jurisdiction.
Principal Identification	Capability	Identifying the Money Laundering Compliance Principal (MLCP), responsible for compliance within an organisation. As well as being a designated contact, this person must also hold a position of seniority within the organisation at board of directors level.

Questions to ask

Area	Key Questions
Coverage	• Which geographies are covered? • What types of organisation are covered?
Quality	• Which sources are used? • How reliable are the data sources? • Are there data quality issues? • What de-duplication, matching and cross-referencing tools are provided?
Efficiency	• What technologies are employed to ensure effective identification and matching of organisations and key people – e.g. advanced analytics? • How does the solution address the risk of false matches? • How efficient are the APIs to data sources?
Maturity	• How has the solution been proven or tested? • What metrics are available on solution performance? • Is there relevant external certification?
Compliance	• What assurances can be given that the solution meets the AML/KYC requirements? • Does the solution comply with relevant data protection laws, including the collection, use and storage of personal data? • What consent is needed from the customer to access this data? • How are Data Subject Access Requests addressed under GDPR?

Identification of individuals

IDENTIFICATION OF INDIVIDUALS CAN BE BROKEN DOWN IN THIS WAY:



Understanding the process

Identify the person

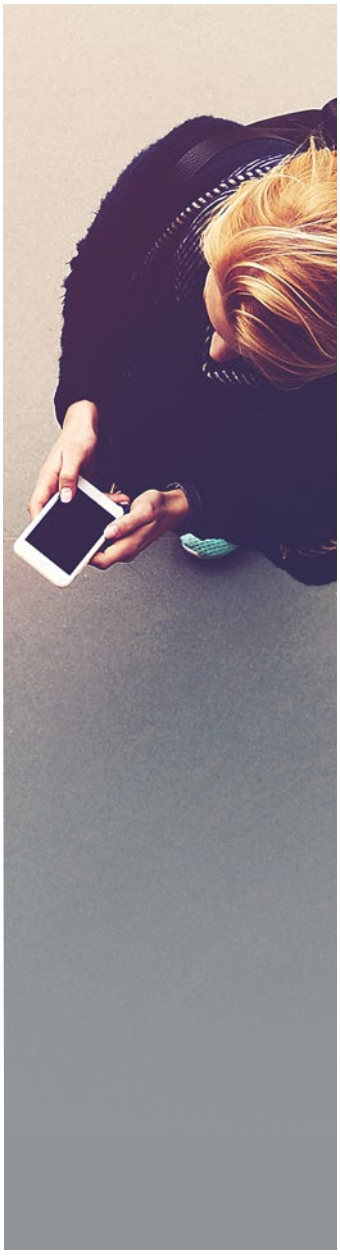
Identity claim
The first step in identifying a person is to know which identity they are claiming, based on the initial identity information they provide, such as name, date of birth and address.

Their claim may be contained in the evidence they provide, for instance a driver's licence may include all of the required information.

Many countries maintain a national register of citizens where a person's national identity number enables the person to claim a unique identity. In the US, the social security number has often been used as a de facto national identity number even though it was not designed for that purpose.

Identity evidence
The next step is to gather evidence to support the identity claim. The nature and quantity evidence required is determined by regulatory requirements but also limited by what is available to the person. This evidence may include:

- Documentary evidence – e.g. documents issued by government bodies or other regulated entities.
- Electronic evidence – typically asking the customer to provide personal information attributes such as name, address and date of birth that can be used in the identity verification process.



Data protection rules may restrict what you can collect, the manner in which it is done, and how and where the evidence is stored and subsequently used. This may require you to obtain consent from the person before collecting or processing their personal information.

New sources of digital identity evidence that may help reduce friction in the identification process include:

- High assurance digital identities, such as those already available in some European countries that create a portable digital identity from either a bank account or government issued electronic identity. Projects are underway to create similar schemes elsewhere such as the TISA-led project in the UK.[8]
- Identification-sharing, where one organisation relies on the KYC performed by another organisation. Until now, this has often been difficult due to the requirements placed on "reporting entities" and issues around liability. The AML bill currently going through the Australian Parliament aims to "expand the circumstances in which reporting entities may rely on customer identification and verification procedures undertaken by a third party". In a similar vein, several banks in the Nordics are seeking to build a KYC utility to avoid the duplication of costs arising from the need for customers to essentially undertake the same KYC checks with every regulated entity that they deal with.

Verify the person

Identity validation

Identity validation is the process of confirming that the identity that is being claimed corresponds to a real, unique and identifiable individual. Validation involves confirming that the evidence is genuine and potentially also corroborating the evidence against other sources at an attribute level.

Identity verification

Identity verification is the process of confirming that the identity being claimed belongs to the individual that is claiming it.

The verification process can be face-to-face, handled remotely, or through a third party vouching for the individual.

Identity compromise

Counter fraud and anti-impersonation checks are used to detect when identities could be fraudulent or compromised, even though identity validation and identity verification processes have been successful. For example, a fraudster could use genuine but fraudulently obtained documents, such as a real passport obtained through a false application.

Counter fraud checks often involve checking databases of known compromised, synthetic or at-risk identities. If an identity is flagged as being at-risk, then the identification process may fail or it may be necessary to perform additional identity validation and identity verification steps to mitigate the risk.

Other checks

The UK government good practice guide GPG45[9] includes the checking of the recent activity of the identity – i.e. not only is the identity known, verifiable and not known to be compromised but there is evidence that the identity has been used without issue by the individual in question.

8 https://www.tisa.uk.com/tisa-groups-projects/digitalisation/

9 https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

Choosing suppliers

Capability	Service Type	Description
End-to-end Process		
Identity Verification Curator	Service	Provides an end-to-end service enabling organisations to verify the identity of individuals. The supplier will have selected the components that make up their end-to-end solution. It is intended to provide a one-stop-shop for identity verification.
Identity Verification Aggregator	Service	Provides an end-to-end service made up of individual components, which the client may select to support them in verifying the identity of individuals. This provides the client with a greater degree of choice when specifying their identity verification requirements. It would also normally imply a greater degree of expertise, required to select their preferred service components.
Video Identification	Service	Taking the individual through the identification process using a live video session with an identification specialist. The process will involve the individual providing information about themselves and presenting documents. The individual may need to hold documents such as passports at different angles so the identity specialist can see the security features in the documents.
Digital Identity Aggregator	Service	Providing access and integration to high assurance digital identities issued by government or private sector digital identity schemes in some countries.
Identify the Person		
Document Verification	Capability	Using digital technology to scan and verify physical documents such as passports and driving licences. Mobile based solutions will use a combination of image capture and reading chips embedded in documents (using NFC). Images will be analysed and compared against reference documents. The processing may include checking the quality of the printing and checking physical security features such as holograms. Often automated checks are supported by manual checks conducted by trained document examiners. Where chips can be read (as is the case with most passports) the information read from the chip can be cryptographically verified as having been issued by a legitimate recognised issuing authority. Hardware-based solutions to verify documents can be used to perform a similar process in a face-to-face environment.
Digital Documents	Capability	Some countries (e.g. the US and Australia) are beginning to roll out digital driving licences. These are provisioned into the individual's mobile phone and will be able to be interrogated directly in order to corroborate the individual's identity. Several European countries issue electronic identity smart cards that provide an authoritative confirmation of identity. These are read using a smart card reader that needs to be connected to the individual's PC. The Nordic countries, Netherlands and Belgium have bank-operated identity schemes, providing individuals with digital identities.

Choosing suppliers

Capability	Service Type	Description
Verify the Person		
Data Source Aggregators	Service	These provide access to numerous data sources that can be employed at several points in the identification process. Sources may include: • Credit bureaux: have access to large amounts of personal data relating to individuals and their transaction histories. • Government sources: have access to large amounts of person data relating to individuals and their dealings with official bodies. Some of this data will be publicly available e.g. electoral roll records. • Watch lists: various lists, maintained by government, law enforcement and regulatory organisations, of known or suspected money launderers, terrorists, or other persons considered high risk. • Social media: publicly available data about individuals, the extent of which depends on their personal privacy preferences and those of their social circle.
Individual Data Sources	Capability	As well as the above data sources, you may want to access additional sources that are available . For example, the new open banking APIs may provide access to details about the payment accounts an individual holds, the associated personal data as well as transaction histories.
Biometric Comparison (against document)	Capability	Biometric comparison involves checking biometrics against details stored on an official document. The most common form of this is comparing the face of an individual to the image on a document that they have presented. The process must include a "liveness" test to prevent attempts to fool the system, e.g. by presenting a photograph of the person. Suppliers may employ different techniques to perform both the comparison and the liveness tests and so care should be taken to assess the robustness of any solution. US government organisation NIST[10] has a programme to assess the quality of facial biometric solutions Biometric comparison can be performed remotely, using a mobile device, or in-person, using a hardware-based solution.
Knowledge-based Verification (static and dynamic)	Capability	Knowledge-based verification[11] aims to demonstrate the individual is who they claim to be, by asking questions that only they should be able to answer. Questions can include: • **Static information:** key information about the individual that does not change, e.g. mother's maiden name. • **Dynamic information:** recent transactions or payments that only the individual will know, e.g. most recent credit card bill. There are significant issues with the quality of knowledge-based verification (KBV). The user experience can be poor and ultimately all of the information is phishable.
Vouching	Capability	Some individuals may not be able provide sufficient evidence to prove their identity. In these cases, it may be possible for a trusted professional, e.g. doctor or social worker, to vouch for the person.

10 https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing

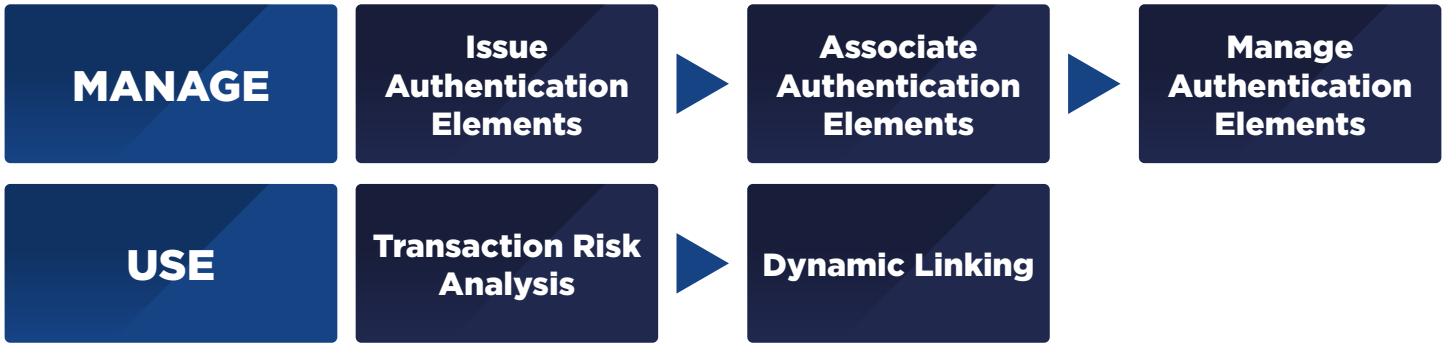
11 Sometimes referred to as "Knowledge- based authentication".

Questions to ask

Area	Key Questions
Coverage	• Which sources are used? • How will does the solution cover your customer base – thinking especially about people with a small financial footprint, who have disabilities, who are less comfortable with technology or who live in remote locations? • How will your customers perceive the solution?
Quality	• How reliable are the data sources? • Are there data quality issues? • What de-duplication, matching and cross-referencing tools are provided? • What assurances can be provided on document verification processes?
Efficiency	• How much friction does the solution place into the user journey? • Is the solution fully digital? How often is it necessary to fall back on manual processes? • How well will the solution work in the channels through which you serve your customers?
Support	• How much visibility and input will you have in the development of the solution? • If you encounter issues with the solution (e.g. it doesn't work well for some of your customers or fraud rates suggest there could be an issue), how much influence will you have in ensuring those issues are addressed? • Is the supplier vulnerable to significant change (e.g. acquisition) that could affect the service offered to you?
Maturity	• How has the solution been proven or tested? • What metrics are available on solution performance? • Is there relevant external certification?
Security	• How resistant to impersonation is the solution, e.g. not reliant on information that can be obtained through phishing or purchased on the dark web? • Is the solution effective at detecting fake or synthetic identities? • How robust are any biometrics processes? Can the supplier provide evidence to support the claimed performance of the technology, e.g. external certification or verifiable performance figures?
Compliance	• What assurances can be given that the solution meets the AML/KYC requirements? • Does the solution comply with relevant data protection laws, including the collection, use and storage of personal data? How is the data stored and processed? When is it purged? • Where sensitive biometric data is being collected how is it being stored or processed? • What consent is needed from the customer to access this data? • How are Data Subject Access Requests addressed under GDPR? • Does the check leave a trace on a credit file? • What audit trails can be provided on checks performed?

Authentication

FOR AUTHENTICATION YOU NEED TO CONSIDER THE FULL LIFECYCLE OF THE AUTHENTICATION ELEMENTS USED BY INDIVIDUALS TO ACCESS SERVICES AS FOLLOWS:



Understanding the process

Manage authentication

Issue authentication elements
For many years the terms "two-factor authentication" or "multi-factor authentication" have been used to describe strong authentication. The idea is that to make authentication more secure multiple independent authentication steps (or "factors") are employed. If one factor is compromised, the other factors will remain and protect against unauthorised access to the service.

PSD2 (the 2nd European Payment Services Directive) formalises the requirement for strong customer authentication in payments[12]. It uses the word "element" instead of "factor" and defines the following element types:

- **Knowledge –** "what you know".
- **Possession –** "what you have".
- **Inherence –** "what you are".

Strong customer authentication requires authentication with at least two of the above elements, which must be independent of each other. Examples might include PIN (knowledge) + card (possession) or passphrase (knowledge) + voice biometric (inherence).

Choosing which elements are best suited to your service and your customers is not trivial. You will need think about which integrate best with your service, giving an optimal user experience whilst achieving the levels of security you need. It is also important to consider the channel in order to determine which factors will work best for your customers, whilst providing the necessary security to mitigate the risks. Mobile, web and messaging should be evaluated against their differing qualities in relation to convenience, cost, flexibility and security.

Associate authentication elements
This is the process of ensuring that authentication elements have been issued to the correct known customer. Sometimes it is referred to as "binding".

Manage authentication elements
Authentication elements have to be managed through their full lifecycle, including issuance, revocation and replacement, as well as ongoing monitoring to mitigate fraud.

Use authentication

Transaction risk analysis
Real time analysis is required to detect:

- Abnormal spending or behavioural pattern of the payer.
- Unusual information about the payer's device/ software access.
- Malware infection in any session of the authentication procedure.
- Known fraud scenario in the provision of payment services.
- Abnormal location of the payer.
- High-risk location of the payee.

Dynamic linking
The authentication is tied to the transaction details (e.g. the amount in a payment) such that the authentication data cannot be captured and replayed in a different context.

12 https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2

Choosing suppliers

Capability	Service Type	Description
End-to-end Process		
Authentication Curator	Service	An end-to-end service, where the supplier selects best of breed authentication elements. Some curators focus on particular channels, e.g. providing an authentication solution for mobile.
Authentication Aggregator	Service	An end-to-end service offering a range of components and the ability to integrate other external authentication elements.
Manage Authentication		
Knowledge Element	Capability	A knowledge element can consist of information that is either: • Secret, such as a password or PIN that the individual is required to not to share with anyone else. • Private, personal information that will normally only be known to the individual such as biographic information or recent transactional history. As with knowledge-based verification (under "Identification of individuals" above), knowledge-based authentication can be either static or dynamic. Passwords and knowledge-based verification often result in a poor experience, the knowledge may be guessable, phishable, available on the dark web or recoverable through brute force.
Possession Element	Capability	A possession element is a physical security token or a device in the possession of the individual. Secured mobile apps are recognised as a means of confirming possession of the phone at that point in time. It should be noted that the European Banking Authority opinion distinguishes between "secure mobile apps" and "mobile apps". Without the necessary levels of security, it may not be possible to determine possession. With reference to device intelligence, some devices may offer features that enable it to determine whether it is still in the possession of its usual owner, such as location tracking and gait monitoring.
Inherence Element	Capability	Inherence refers to biometrics of which there are many types, falling into two main categories: • Physiological, a physical characteristic such as fingerprint, iris, face or voice.[13] • Behavioural, a behavioural characteristic such as the way the individual interacts with a device (e.g. keystroke patterns, how the device is held) or how they speak. Mobile biometrics checks may be performed on the mobile device or in a remote server. You will need to consider what biometric data is being captured and where it is being processed and stored, in order to comply with data protection requirements. Hardware solutions, such as finger vein readers, may be appropriate for business customers where the cost of such hardware can be justified.
Use Authentication		
Transaction Risk Analysis	Service	Advanced Analytics is an essential part of transaction risk analysis. Machine Learning is increasingly popular in this context, in order to gain the best possible balance between a frictionless user experience and fraud prevention requirements. Device fingerprinting is also a key aspect of managing risk, recognising when a customer is connecting from a known device and location. Access from an unexpected IP address on an unexpected device in an unexpected location is clearly worth investigating.

13 Voice can be viewed as physiological (determined by the shape of the vocal tract) and behavioural (including speech cadence, inflection and accent)

Questions to ask

Area	Key Questions
Coverage	• How will does the solution cover your customer base – for example, if the solution is mobile-based, is that suitable for all your customers? • How will your customers perceive the solution?
Efficiency	• How much friction does the solution place into the user journey? • How well will the solution work in the channels through which you serve your customers?
Support	• How much visibility and say will you have in the development of the solution? • If you encounter issues with the solution (e.g. it doesn't work well for some of your customers or fraud rates suggest there could be an issue) how much influence will you have in ensuring those issues are addressed? • Is the supplier vulnerable to significant change (e.g. acquisition) that could affect the service offered to you? • Do mobile solutions work equally well on Android and Apple devices?
Maturity	• How has the solution been proven or tested? • What metrics are available on solution performance? • Is there relevant external certification?
Security	• Is the solution resistant to account takeover and other common attacks? • Does the solution include fraud detection and prevention measures, such as monitoring unusual behaviour? What happens when fraud is suspected? • How robust are any biometrics processes? Can the supplier provide evidence to support the claimed performance of the technology, e.g. external certification or verifiable performance figures? • Does the solution provide an alternative to or mitigate the risks[14] with sending one-time codes over SMS?
Compliance	• What assurances can be given that the solution meets the PSD2 SCA requirements? • Does the solution comply with relevant data protection laws, including the collection, use and storage of personal data?

14 There are widely publicised issues with SMS including "SIM Swap" and vulnerabilities in the SS7 protocol that underpins the mobile networks.

Appendices

Project Financial Crime Benefactor

Refinitiv

Refinitiv is one of the world's largest providers of financial markets data and infrastructure, serving over 40,000 institutions in approximately 190 countries. It provides leading data and insights, trading platforms, and open data and technology platforms that connect a thriving global financial markets community – driving performance in trading, investment, wealth management, regulatory compliance, market data management, enterprise risk and fighting financial crime.

Qual-ID' combines digital ID verification and document proofing from Trulioo with risk screening from World-Check in a single point of access. Qual-ID is designed to improve the consumer experience while helping to protect against fraud and money laundering.

It supports a fast and secure way to digitally onboard consumers through a combination of Refinitiv's World-Check Risk Intelligence with Trulioo's digital identity network. Qual-ID enables organisations to verify identities against trusted data sources, proof legal documents, conduct anti-impersonation checks, and screen for regulatory and financial risk; such as sanctions, PEPs and adverse media. The process can be completed in one transaction and via a single point of access.

Use of Refinitiv Qual-ID comprises three steps:

- Identity Verification (IDV): Verifying that a person actually exists and that they are who they say they are by comparing attributes provided with information obtained from independent trusted sources such as governments, and credit bureaus.
- Identity Proofing (IDP): Answering the question 'Is this identity document legitimate?' A facial comparison element adds additional assurance and both automated algorithmic and manual checks are available to increase effectiveness. An anti-impersonation check can be performed though a second layer of biometric authentication using a live "selfie" via a mobile device and a liveness check is performed to ensure they are not holding up a photo.
- Risk Screening: Access to Refinitiv's Risk Intelligence data via World-Check, enabling comprehensive customer screening.

James Mirfin, Head of Digital Identity and Financial Crime Propositions
james.mirfin@refinitiv.com
www.refinitiv.com
www.refinitiv.com/qual-id

Author

Consult Hyperion

Consult Hyperion is an independent strategic and technical consultancy, based in the UK and US, specialising in secure electronic transactions. With over 30 years' experience, we help organisations around the world exploit new technologies to secure electronic payments and identity transaction services. From mobile payments and chip & PIN, to contactless ticketing and smart identity cards, we deliver value to our clients by supporting them in delivering their strategy. We offer advisory services and technical consultancy using a practical approach and expert knowledge of relevant technologies. Hyperlab, our inhouse software development and testing team, further supports our globally recognised expertise at every step in the electronic transaction value chain, from authentication, access and networks, to databases and applications.

www.chyp.com
pressoffice@chyp.com

Project Financial Crime Members

Kompli-Global Ltd.

Kompli-Global has developed specialist corporate due diligence solutions comprising of unique proprietary products, linked to best in class third party services to deliver the most comprehensive, international customer risk screening, on-boarding and on-going monitoring.

Martin Pashley, Director and Chief Commercial Officer
martin.pashley@kompli-Global.com
www.kompli-global.com

GBG

GBG is a global specialist in identity and location data intelligence, and anti-fraud and compliance solutions. Our innovative technology is built on an unparalleled breadth of data obtained from over 200 global partners, helping us verify the identity of over 4.4 billion people worldwide.

Jonathan Jensen, Commercial Director Identity
jonathan.jensen@gbgplc.com
www.gbgplc.com

Buguroo

Buguroo combines deep learning along with behavioural biometry to detect known and unknown malware and alert for any anomalous behaviour during the entire session, detect banking fraud before it happens.

Tim Ayling, EMEA Vice-President
tayling@buguroo.com
www.buguroo.com

EPA Members

Ozone Financial Technologies Ltd

Huw Davies, Co-founder and Chief Commercial Officer
huw@ozoneapi.com
www.ozoneapi.com

W2 Global Data Solutions Ltd

Gary Pine, Chief Product & Marketing Officer
Gary.pine@w2globaldata.com
www.w2globaldata.com

Appreciate Group plc

Julian Coghlan, Chief Commercial Officer
julian.coghlan@appreciategroup.co.uk
www.appreciategroup.co.uk

Contis

Jason Ollivier, Chief Disruption Officer
jason.ollivier@contis.com
contis.com

Moorwand

Philippa Artus, Marketing and Projects Manager
pa@moorwand.com
www.moorwand.com

Kemp Little

Chris Hill, Partner and Head of Fintech
chris.hill@kemplittle.com
www.kemplittle.com

Paragon ID

Angela Davies, Business Development
Angela.Davies@paragon-id.com
www.paragon-id.com

XTN Cognitive Security®

Guido Ronchetti, Chief Technical Officer
guido.ronchetti@xtn-lab.com
xtn-lab.com

Eversheds Sutherland LLP

Richard Jones, Partner and Head of Payments Services
richardjones@eversheds-sutherland.com
www.eversheds-sutherland.com/global/en/where/europe/uk/sectors/financial-institutions/payment-matters.page

JudoPay

Charlotte Karg, Payment Consultant
charlotte.karg@judopay.com
www.judopay.com

K & L Gates, LLP

Judith Rinearson, Partner
judith.rinearson@klgates.com
www.klgates.com

Okay

Fabien Ignaccolo, Chief Executive Officer
fabien@okaythis.com
www.okaythis.com

PXP Financial

contact@pxpfinancial.com
www.pxpfinancial.com

Entersekt

Simon Rodway, Senior Pre-sales Consultant
srodway@entersekt.com
www.entersekt.com

Protean Risk Ltd

Tristan Sargeaunt, Director of Fintech & Payment Services
tristansargeaunt@proteanrisk.com
www.proteanrisk.com

twenty8k consulting

Ian Staniforth, Director
ian.staniforth@twenty8k.consulting
www.twenty8k.consulting

Post Office

Jim Purves, Consultant
identity.sales@postoffice.co.uk
www.postoffice.co.uk/identity

Emerging Payments Association

The News Building,
3 London Bridge Street,
SE1 9SG, UK

Tel: +44 (0) 20 7378 9890

Web: emergingpayments.org

Email: info@emergingpayments.org

@EPAssoc

Emerging Payments Association