payments
strategy
forum

June 2017

Guidelines for Identity Verification, Authentication and Risk Assessment – Guidelines Scope

Document Context:

This document was finalised in June 2017 as part of the Guidelines for Identity Verification, Authentication and Risk Assessment workstream activities. This document will be used as deliverable for handover. This document provides a detailed description of the proposed scope of the guidelines.

FINAL V1.0 19th June 2017

GUIDELINES FOR IDENTITY VERIFICATION, AUTHENTICATION AND RISK ASSESSMENT

SCOPE OF GUIDELINES TO BE DEVELOPED AND IMPLEMENTED

Contents

Preface

This document has been produced as part of implementing the ‘Payments Strategy for the 21st Century’, developed and published by the Payments Strategy Forum in November 2016. It has been prepared by the Financial Crime, Security and Data Working Group in connection with developing solutions to ’Improving Trust in Payments’.

Overview of Purpose, Usage and Benefit of Guidelines

The main purpose of the Guidelines are to reduce confusion and increase consistency of understanding, interpretation and application of the significant number of existing regulations and other official guidance associated with verifying the Payer (source of payment) and Payee (receiver of payment) identities when making payments.

It is expected that these will be used mainly by Payment Service Providers (PSPs), particularly smaller organisations and new entrants, to inform and simplify their approach to understanding regulatory requirements/guidance and adopting a consistent approach to end-user identification when making and receiving payments. This will strengthen overall industry Identity Management control and effectiveness, contributing to a reduction in the detriments identified as part of the Payments Strategy work.

End-users (e.g. Consumer, Charity/Not for Profit Organisations, Business and Government users of Payments Services) may also benefit through having a reference that provides a common language and understanding of the elements of identity verification that impact them when making and receiving payments.

Objective of This Document

This document sets out the scope of the Guidelines in order that detailed drafting can commence prior to testing and validation with a broader stakeholder community. The principle adopted is that the Guidelines will apply to all electronic payments made through any channel (e.g. in-store, online, by telephone) processed by PSPs operating in the UK. They will comprise:

- key attributes of an end-user’s identity (e.g. name, address);
- steps and further information gathering taken by PSPs to confirm (verify) the identity of the end-user (e.g. information from validated credentials such as passports and driving licences);
- methods used by PSPs to authenticate the payment request (e.g. that it has been made by the person whose identity has been previously verified);
- approaches taken by PSPs to make a risk-based judgement regarding whether or not to make the payment based on the verification/authentication outcomes.

Also included is guidance on exemptions and specific regulatory requirements, including chapter references where relevant. No additional obligations are incorporated into the guidance.

Chapter 1: Key Regulations, Legislation and Guidance

- 4th Money Laundering Directive (4MLD)
- Payment Services Directive 2 (PSD2)
- EBA PSD2 Strong Customer Authentication (SCA) Regulatory Technical Standards (EBA RTS)
- Joint Money Laundering Steering Group Guidance (JMLSG)
- UK HM Government guidance (GOV.UK)
- FCA Financial Crime Guide (FCAFCG)
- European Electronic Trust Services Regulation (eIDAS)
- EU Funds Transfer Regulations (WTR2)
- UK Data Protection Act (DPA)
- EU General Data Protection Regulations (GDPR)
- BSI Digital Identification and Authentication code of practice (PAS499)
- UK Money Laundering Regulations 2007 (MLR)
- UK Payments Accounts Regulations 2015 (PAR) and EU Payments Accounts Directive 2014 (PAD)
- UK Current Account Switching Service (CASS)

Chapter 2: Applicability of Guidelines

This chapter will define the applicability of the Guidelines by:

- Type of firm (Payment Service Provider - PSP)
- Type of customer (Payment Service User - PSU)
- Type of payment or action/transaction (electronic only)

It will describe and clarify the alignment with other current and planned guidelines, regulations and related activities.

Whilst the Guidelines must be written to cover all Payments Service Providers, they are likely to be most helpful to smaller or less established firms, including those that are providing intermediary services such as Account Information Service Providers or Payment Initiation Service Providers.

The initial implementation of the Guidelines should be limited to identity management of Payment Service Users who are ‘natural persons’ (e.g. private individuals, including those acting as sole traders). Whilst not currently planned, the Guidelines could feasibly be subsequently extended to include PSUs who are partnerships and companies (‘juridical persons’). This will, however, add a significant degree of complexity and should be balanced with the additional benefits for the target audience.

The Guidelines are not intended to be used for PSPs to identify each other, as this will be an inherent part of the establishment of the mechanism used by the PSP to undertake payments related services and covered by specific processes, regulations and guidelines.

The Guidelines are intended to be used by PSPs that are processing payments that are electronic rather than based on underlying physical instruments such as cash or cheques, but they should not be restricted by the channels used to initiate and complete the payment (e.g. by telephone). They are however restricted to PSPs operating in the UK and subject to, inter alia, UK law.

Although the Guidelines are focussed on the activities of: acquiring customers; initiating payments; post-payment interactions; and ongoing account management for the majority of payments (including card based), they are likely to be helpful for managing the identity aspects of many interactions between Payment Service Providers and their Payment Service Users. For example, the Guidelines will also be relevant for non-payment specific activities such as conducting a transaction with a risk of fraud or misuse, such as changing the address on an account.

The Guidelines are not intended to replace or contradict any existing guidance or to add any additional obligations beyond that set out in applicable regulations and legislation. The Guidelines are based on existing and proposed regulations, legislation and guidance and will include references to existing material where appropriate.

Illustrative (partial) content

These guidelines apply to all electronic based payments processed by payments service providers operating in the UK.

They do not apply to other forms of payment such as cash or cheque, even if the cheque is converted to an electronic image for depositing.

The guidelines apply to electronic payments made by any mode (e.g. in-store, in-branch, online, by telephone).

Chapter 3: Exemptions

This chapter will set out where the Guidelines are less applicable or not appropriate to be used. It will also highlight regulatory provisions where identity verification and authentication is not required, but where the Guidelines and associated risk-based approach may still be helpful (e.g. post transaction fraud reporting).

Examples of exemptions that should be highlighted in this chapter include:

- In accordance with 4MLD Art 11(b)(ii) customer due diligence is required with respect to occasional fund transfers over EUR 1,000. This is consistent with the Regulation on the information accompanying transfers of funds (WTR2) which permits that the payer and payee information associated to transfers less than EUR 1,000 need not be subject to verification.
- Remote electronic payments (e.g. when initiating an online payment or payment via a mobile device) not exceeding EUR 30 are exempt from SCA requirements (EBA RTS Art 15).
- Re-authentication is only mandatory when, since SCA was last applied to the PSU, the cumulative amount of transfers exceeds EUR 100, or the user has already undertaken five remote electronic payment transactions (EBA RTS Art 15).
- A payment service provider's policies and procedures must set out the circumstances in which it will not seek to verify user identities under a permitted risk based approach.

Illustrative (partial) content

A PSP's policies and procedures should clearly articulate any exemptions from customer identity verification it chooses to utilise. Firms are not bound to avail themselves of exemptions; therefore firms need to make such decisions within their risk-based approach.

Chapter 4: ID&V Policies and Procedures

This chapter will set out requirements that will ensure consistent content topics and review processes are incorporated across PSPs, when they are complying with the obligation that their internal financial crime policies and procedures should clearly articulate their approach to user identity management.

The emphasis for this chapter is on identity verification rather that the broader KYC obligations, however the linkage with those needs to be clear and appropriate. The policies need to include appropriate risk appetite statements and set out the procedures that are in place to monitor and review these, as well as the governance regarding compliance and approval of any waivers or exceptions.

To promote consistency of approach, especially when users are considering the extent to which they could place reliance on identity verification that has been undertaken by another PSP, consideration should be given to the Guidelines including a requirement for a standard risk assessment template to be used, covering a minimum set of risk factors to be incorporated into PSP policy and procedures relating to ID&V.

Illustrative (partial) content

PSPs should establish appropriate internal policies and procedures regarding the establishment and verification of user identities. These are likely to form part of the firm's broader financial crime compliance policies and procedures and the ownership of the ID&V related policies and procedures should be clear. The policies and procedures should be reviewed at least annually and in response to material changes in the nature of the firm's business or the external operating environment to ensure continued appropriateness.

Chapter 5: Concept and Components of Identity

This chapter will set out the attributes related to a payment service users identity which might be gathered, validated and verified (e.g. name, date of birth, address, nationality, gender, finger print, voice pattern, retina, heart rhythm)

It will include references to JMLSG Part 1 Chapter 5.3 which addresses the 'standard evidence' to be obtained. It must also cover non-standard evidence that may be used where the standard evidence is not available, taking into account a risk based approach.

Whilst the (initial) scope of these Guidelines are for identity verification for non-corporate PSUs, the CMA Retail Banking remedy regarding SME Business Current Account opening should be reviewed as the majority of SME are sole traders which are included in the scope of the Guidelines.

Illustrative (partial) content

PSPs should decide which attributes related to a user's identity they will seek to verify in order to achieve the level of certainty determined to be appropriate under the firm's risk-based approach.

The policies and procedures should clearly set out: the identity information to be collected from users; the aspects of that identity information that require validation; the aspects of that identity information which require verification; the level of identity assurance required in accordance with the firm's risk appetite.

Chapter 6: Identity Management Components

This chapter will outline the common components of identity management (irrespective of firm, customer or payment type):

- Identity Information Gathering: Enable a user to assert an identity by the collection of a defined set of identity related attributes;
- Identity Validation: Establish that asserted identity is genuine/valid by means of independent checking of identity attributes;
- Identity Verification: Connect the genuine/validated identity to the user asserting the identity by independent evidence (e.g. matching passport photograph, PSP records)
- Identity Assurance: Establish usage profile of identity (e.g. social media, electoral roll, credit footprint, fraud checks, interaction with public services and utility providers)
- Authentication: establish appropriate risk based mechanisms for the identity assured user to securely confirm authorisation of transactions
- Secure transmission and storage of identity attributes

The Guidelines should draw on and reference GOV.UK Good Practice Guide GPG44 and GPG45 as implemented by GOV.UK Verify

Illustrative (partial) content

The following is a summary of the key stages of identity management that all PSPs must implement:

- Identity information gathering: the process deployed by a PSP to enable an applicant to assert an identity.
- Identity validation: the process of determining that the identity asserted by the applicant is a genuine identity.
- Identity verification: the process of establishing an evidential connection between the asserted genuine identity and the applicant.
- Identity assurance: the process of gathering evidence to confirm the claimed identity is active and not known to be fraudulent.
- Authentication: the process of checking credentials supplied by a user that is initiating a transaction to confirm they originate from the assured identity.
- Secure records storage: the process of ensuring that identity data is sent and stored securely to prevent interception or loss and provide a retrievable audit trail.

Chapter 7: Identity Management ‘Events’

This chapter will set out the points in the customer and/or transaction lifecycle at which identity management beyond the authentication of routine transactions is appropriate. For example, this would include: the commencement of a customer relationship; prior to a one-off non routine transaction; for transactions over a specified value; once a certain aggregate payment value is reached; on a periodic basis; if the account becomes dormant. Some of these events will trigger more in depth identity management (e.g. account opening).

The section draws on:

- JMLSG Guidance
- PSD2 SCA Regulatory Technical Standards
- MLR Regulations 7 and 8
- WTR2

Illustrative (partial) content

A PSP must determine the points in the customer lifecycle at which it is appropriate to verify and subsequently re-verify customer identities.

Identification verification or authentication must be applied when a PSP:

- establishes a new customer relationship;
- suspects money laundering or terrorist financing;
- doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.
- processes a remote electronic payment (e.g. when initiating an online payment or payment via a mobile device) greater than EUR 30;
- has identified that a customer has initiated a cumulative total of EUR 100 or 5 remote electronic payments since customer authentication was last applied;
- has first contact with a customer following 12 months of inactivity (dormancy);
- has identified material changes in the customer’s payment pattern;
- engages in a remote action with a significant risk of fraud or misuse;
- contacts the customer to discuss secure aspects of their account with them.

It is important that PSPs are able to monitor users’ cumulative activity and identify linked operations.

Chapter 8: Identity Validation and Verification Methods

This chapter will outline the different options for validating and verifying identity attributes:

- Documentary (originals in a face-to-face situation, certified copy documents in a non-face-to-face situation)
- Electronic verification as articulated in the proposed 2017 JMLSG Guidance
- Digital Identity assurance mechanisms (e.g. trust certificates, digital passports), also in line with the proposed 2017 JMLSG Guidance
- Biometrics (retina, fingerprint, voice etc.)
- The section draws on and references:
- JMLSG Guidance Part 1, Chapter 5.3
- GOV.UK Good Practice Guide GPG45 re digital ID and IDP processes
- 4MLD (and the 5th revision under development)

Illustrative (partial) content

PSPs must select, and incorporate into their procedures, identity validation and verification methods which are appropriate to the nature of the business, type of customer and delivery channels concerned.

PSPs should retain records evidencing the factors considered when assessing the chosen method(s) and the rationale for selecting them.

A PSP may choose to use multiple identity validation and verification methods (e.g. for different customer types or distribution channels) but must be alive to the risk of inconsistency and variable standards.

Chapter 9: Risk-Based Approach

This chapter will reinforce that payment service providers are expected/required to take a risk-based approach to customer due diligence, including authentication, identification and verification.

Risk variables regarding identity include:

- the breadth of evidence
- the strength of the evidence
- the validation and verification processes carried out
- a history of the user's activity and behaviour
- user-related data, for example where a customer is a Politically Exposed Person

The Guidelines will note that whilst there are other risk factors/variables which firms must consider under their broader risk-based approach (e.g. country risk, product risk, distribution channel risk), the risk variables set out in this section concentrate on the risk of identity misuse (which is the harm or detriment that the guideline seeks to address).

This section should also cover indirect as well as direct identity risk assessment – for example where a PSP (e.g. bank) provides services to another PSP (e.g. Money Service Bureau) both will need to have a clear position on PSU identity risk appetite. The Guidelines should be capable of being used as the basis of a common framework for the (for example) MSB to articulate and demonstrate a level of risk appetite and control that is acceptable to (for example) the bank, to allow them to support the provision of services on an agreed risk based approach. Whilst outside the scope of the Guidelines, this should also reference the need to clear about and agree relative liabilities for fraud losses or compliance breaches.

The section draws on:

- FCA Financial Crime Guide (which calls for a risk-based approach)
- Money Laundering Regulations 2007 (which require risk-sensitive customer due diligence)

- JMLSG Part 1, Chapters 4 and 5
- GOV.UK Verify, GPG 45
- eIDAS Regulation

Illustrative (partial) content

The following is based on the framework set out in GPG 45

Level 1 identity – the applicant supplies an identifier which must be confirmed as being in existence and in the possession/control of the applicant. No validation, verification, counter fraud checks. No requirement to prove the activity associated with the identity. It is recommended that Level 1 identities do not carry sufficient certainty for payment service providers to be 'reasonably satisfied' as to the identity of their customer (N.B. the JMLSG Guidance repeatedly refers to the need for firms to be reasonably satisfied as to customer identity).

A Level 2 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the Applicant is owner of that identity might be offered in support of civil proceedings (i.e. identity is established 'on the balance of probability').

A Level 3 Identity is a Claimed Identity with evidence that supports the real world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken to determine that the identity relates to a real person and that the Applicant is the owner of that identity might be offered in support of criminal proceedings (i.e. identity is established 'beyond reasonable doubt').

A Level 4 Identity is a Level 3 Identity that is required to provide further evidence and is subjected to additional and specific processes, including the use of Biometrics, to further protect the identity from impersonation or fabrication. It is recommended that Level 4 identities are not generally necessary for the purposes of payment service providers, unless there is a particular doubt about the identity evidence or there are indicators of particularly elevated financial crime risk.

Research conducted for the Open Identity Exchange shows that identity verification steps taken by financial institutions undertaking account opening broadly correspond to Level 2 identities. However, a number of financial institutions have indicated an intention to move towards Level 3 identities.

Ultimately, it is for a PSP to determine, under its risk based approach, how much certainty of customer identities it requires.

Chapter 10: Multi-factor Authentication

This chapter will include a high-level description of multi-factor authentications:

- Knowledge factors
- Inherence factors
- Possession factors

This will be based on and reference PSD2 (EBA) SCA Regulatory Technical Standards and 4MLD Art 4(1)

Illustrative (partial) content

PSPs must only issue authentication codes (e.g. a one-time use only numeric code to complete an online payment) to their customer when they have satisfied themselves that they have confirmed the user's identity using at least two of the following three authentication factors:

- Knowledge factors - where a payment service provider gains comfort as to the user's identity as the user is able to demonstrate knowledge of information that only the true owner of the identity would likely know (e.g. mothers maiden name, recent transactions).
- Inherence factors – which relate to the inherent characteristics or attributes of the user. Biometric evidence (e.g. retina, fingerprint, voice pattern, heart rhythm) fall within this category. The security as to identity comes from the fact that these inherent characteristics are hard (if not impossible) to change and forging them is a high barrier to entry to criminals.
- Possession factors – which rely on the user being in possession of identity related device or tokens (e.g mobile phone, security key generator).

Two-factor authentication is in common usage, for example, when withdrawing cash, which requires a bank card (possession) and a PIN number (knowledge).

It is for a PSP to determine which factors are appropriate to achieve strong customer authentication.

Chapter 11: Risk Assessment

This chapter will emphasise that transactions (both outbound and inbound) should not be processed unless a risk assessment which incorporates user identities is conducted. PSPs might choose to decline transactions where they do not have sufficient comfort as to the identities of the parties involved.

Reference will also be made to the PSD2 Regulatory Technical Standards

Illustrative (partial) content

The EBA RTS support taking a risk-based approach through the inclusion of SCA exemptions based upon transaction-risk analysis (e.g. the majority of contactless payments under EUR 50 do not require SCA).

An electronic payment transaction is identified by the EBA RTS as posing a low level of risk and not requiring SCA only where the following conditions, in combination with the existing mandatory real time risk analysis, are met:

(i) no abnormal spending or behavioural pattern of the payer has been identified;

(ii) no unusual information about the payer's device/software access has been identified;

(iii) no malware infection in any session of the authentication procedure has been identified;

(iv) no known fraud scenario in the provision of payment services has been identified;

(v) the location of the payer is not abnormal;

(vi) the location of the payee is not identified as high risk;

(vii) the individual is not on any sanctions, AML, PEPs lists.

Chapter 12: Financial Inclusion

This chapter will set out that Payment Service Providers should be prepared to accept alternative forms of identity evidence where users cannot reasonably be expected to provide standard evidence, for example PSUs who are non-UK nationals. This should also include situations where the PSU is represented by an individual with a Power of Attorney (PoA) or other authority to act on the customer's behalf, covering the identity requirements of both parties, recognising the inherent vulnerability for both the PSU and the authority holder.

The particular circumstances where standard evidence may not be available are wide ranging and various regulations set out obligations on the basis of non-discrimination (e.g. UK Payment Account Regulations para 23); financial inclusion (e.g. UK MLR 2017 Regulation 36(3)) or inability (e.g. FCA SYSC Sourcebook section 6.3.7). The JMLSG (Chapter 5.3) provides a number of specific reasons why standard identity evidence may not be available and possible treatments, which should be referenced in the Guidelines.

The Guidelines also need to take into account the broader need to protect against financial exclusion and in particular the narrative and recommendations of the March 2017 House of Lords Select Committee on Financial Exclusion report relating to identity and address verification issues. The referenced FCA Occasional Paper 17 on Access to Financial Services in the UK published in May 2016 should also be reviewed and its observations and findings taken into account.

Illustrative (partial) content

Where a PSP determines a user to be financially excluded, a record of the reasons for so doing must be retained.

A PSP must include a in their policy statements a commitment to considering alternative forms of identification that support financial inclusion, subject to an agreed risk based approach. This information should, subject to the need to ensure the information does not advantage fraudsters, be clearly and consistently communicated to PSUs, PoA holders and relevant advisors through appropriate channels (e.g. branch, telephone, online).

Chapter 13: Managing Identity Verification Difficulties

This chapter will cover options to address issues that may be encountered when verifying identities, for example:

- Accept a less 'certain' identity on an exceptional basis, subject to appropriate governance and taking into account the need for financial inclusion
- Terminate/decline relationship/transaction if the identity cannot be verified to an appropriate degree of certainty
- Consider whether there are grounds for a Suspicious Activity Report (SAR)

This will incorporate requirements under:

- MLR Regulation 11
- UK Payment Account Regulations
- EU Payment Account Directive

Illustrative (partial) content

A PSP's policies and procedures should provide for dealing with situations where it is difficulty to satisfactorily establish a user's identity. Typical options include: accepting a lower level of identity on an exceptional basis (subject to appropriate internal governance); restricting the activity which the customer is permitted to undertake (e.g. only certain payment types, value limits, frequency limits, and geographic limits).

An inability to establish identity might cause a PSP's employees to become suspicious of money laundering or terrorist financing, in which case, it should be considered whether a suspicion report is required.

Ultimately, if a PSP is not reasonably satisfied as to the user's identity, the relationship must be terminated.

PSPs are advised to maintain logs of identities accepted on an exceptional basis and also instances of declines or terminations.

Chapter 14: Reliance on Identity Verification by Another PSP

This chapter will set out common descriptions for the ID&V processes that are used by PSPs to confirm a user's identity and also the sending PSP's level of assurance (confidence) associated with the user's identity.

It will include the requirement for sending PSPs to transmit ID&V descriptors/identifiers as part of information accompanying the user details provided, together with details where the sending PSP has used non-standard evidence or processes for inclusion purposes, and thus enable receiving PSP to decide whether to rely entirely, supplement or undertake own ID&V.

This will chapter will include references to:

- ML Regulation 17
- JMLSG Guidance Part 1, Chapter 5.6
- Data Accompanying payments (Wire Transfer/Funds Transfer Reg)
- And potentially the Current Account Switching Service guidelines

Illustrative (partial) content

To facilitate reliance, PSPs must be equipped to communicate information to the receiving PSP including: verified customer identity; the level of identity assurance achieved; the identity verification method(s) applied; the date of the most recent customer identity authentication.

These guidelines envisage the use of a standardised set of descriptors which can be transmitted alongside payment user information. This then enables the intermediary or payee's PSP to evaluate the identity risk related to the transaction they are seeking to complete.

Chapter 15: Secure Transmission and Storage of Identity Information

This chapter will address the relationship between identity information and 'personal data' and include minimum retention periods.

The Guidelines must cover all forms of information that have been used in the identity verification, authentication and risks assessment processes, both physical and electronic.

The transmission of information Guidelines should be broad enough to cover both existing mechanisms (e.g. physical media) and potential future methods of transferring information (e.g. via cloud based repositories).

Technical detail should be avoided and the sources of requirements should be referenced where appropriate for further information.

The section draws on:

- ML Regulation 19
- Data Protection Act
- GDPR
- JMLSG Guidance Part 1 Chapter 8

Illustrative (partial) content

Records of identification evidence provided or acquired (including metadata) must be kept for a period of at least five years after the relationship with the customer has ended. The date the relationship with the customer ends is the date the business relationship ended, i.e. the closing of the account or accounts. When there is no relationship with the customer other than to make a specific transaction, the five year period starts when the transaction, or the last in a series of linked transactions, is carried out.

Retention may be by way of original documents, hard copies or digital/electronic copies.

Personal data should only be gathered where the data controller has a demonstrable purpose for gathering it. Further, data controllers should only retain such information for as long as the purpose remains valid.

Chapter 16: Steps Following Identity Management

This chapter will cover other financial crime risk management processes that depend upon the users identity, for example name screening processes for sanctions, PEPs and adverse media purposes.

As these guidelines are focussed on identity verification and authentication, they do not specifically address additional processes which utilise identity information.

Specific references that could be included are:

- JMLSG Guidance, Part 3 Chapter 4 on compliance with the UK financial sanctions regime.
- FCA Financial Crime Guide Part 1, Box 7.3 and Part 2, Boxes 8.2 and 8.6 which cover sanctions screening
- MLR Regulation 20(2)(c) which requires that firms' policies and procedures must include means to determine whether a customer is a Politically Exposed Person.

Illustrative (partial) content

Payment service providers are responsible for determining, in line with their risk-based approach, how they comply with legal obligations and regulatory expectations to identify PEPs, avoid sanctions breaches and take account of adverse allegations.

Comfort as to a payment service user's identity can support the effectiveness of name screening processes.

Additional identity information (which may or may not have been subject to verification) might be used to determine whether matches reported by automated name screening are genuine or not.

Chapter 17: Mutual Authentication

This chapter will emphasise that given the number of scams wherein criminals impersonate payment institutions (and vice versa) in order to deceive payment service users into revealing information or transferring funds, users are entitled to a high level of confidence that contact from a payment service provider is genuine and legitimate. It will include guidance regarding suitable methods of providing the PSU with that confidence.

Payment Service Providers also need comfort as to the identities of other PSPs with which they interact during the provision of the payment services (e.g. payer's PSP interacting with an intermediary PSP acting on behalf of the PSU, which then interacts with the payee's PSP). This aspect is outside the scope of the initial guidelines; however it should be referenced as a requirement in the EBA PSD2 RTS which contains specific and detailed provisions including, for example, certificates for electronic seals (Section 2).

Reference will also be made to other aspects of the PSD2 Regulatory Technical Standards.

Illustrative (partial) content

PSPs should be responsible for providing a clear and consistent means of identifying and authenticating themselves to their customers and other PSPs over all communication channels (Internet, Voice, SMS). It is vital that whatever mechanism is used to perform this, it should easily and quickly enable a customer or PSP to differentiate/spot a malicious communication from a legitimate one. For example, providing a call-back number for a customer to use, or providing account information that only the PSP and user would know.

Chapter 18: Outsourcing/Use of Agents

This chapter covers the principles relating to the use of third parties by a PSP to undertake elements of the identification, authentication and risk assessment processes. It recognises that this usage may relate to a specific task or component of the process, or be a part of a wider outsourcing arrangement. It will be important to stress that the Guidelines do not preclude such use of third parties.

An example of the principles is that the contracting PSP retains its accountability for compliance irrespective of any contract provisions and that it is responsible for monitoring the contractor's performance and controls.

Illustrative (partial) content

PSPs may outsource or contract part or all of their processes associated with identity verification and authentication, however they will retain accountability for compliance and associated liabilities. When selecting a third party supplier the PSP must assess suitability using a documented risk based approach.

As part of the contracting process for the selected supplier, a comprehensive Service Level Agreement must be prepared that clearly sets out the various parties responsibilities, accountabilities and when they must be consulted or informed. This document should also be used as the basis of a comprehensive compliance and performance monitoring regime.