Guidelines

Voluntary guidelines and encouraged market behaviours under PSD2 in the 'transitional period'

The following voluntary guidelines and encouraged market behaviours have been prepared by a number of industry bodies to increase customer protection around the practice widely termed 'screen scraping', which is used in the market as a method of accessing customer data or initiating payments on a customer's behalf.

These voluntary guidelines are not legally binding and have been created for Account Servicing Payment Service Providers (ASPSPs), firms that offer Account Information/ Payment Initiation Service Providers (AISPs and PISPs) and Technical Service Providers (TSPs) including regulated firms and businesses relying upon the pre-12 January 2016 grace period (see below for further detail). These guidelines give guidance during the period (the transitional period) between 13 January 2018 when the revised Payment Services Directive (PSD2) came into force[1], and 14 September 2019 when the EBA's Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication (RTS) will apply.

The main aims of these voluntary guidelines are to foster a collaborative and cooperative industry ecosystem around account information services and payment initiation services, and to further boost customer protections. There are significant benefits for all parties in abiding by these voluntary guidelines. ASPSPs will gain additional certainty, security and protection with enhanced protection for their customers. AISPs and PISPs will benefit from smoother and easier access to ASPSP accounts and as with ASPSPs, their customers will benefit from enhanced protection.

- Scope and clarity of these guidelines: These voluntary guidelines and encouraged market behaviours are for all parties active in the market of providing services to customers or providing technical services for account information or payment initiation services (as described under PSD2). Such parties are defined by PSD2 as Account Servicing Payment Service Providers (ASPSPs) i.e. payment account service providers, Account Information Service Providers (AISPs) and Payment Initiation Service Providers (PISPs). The scope of these guidelines includes all firms that are registered/authorised by the Financial Conduct Authority (FCA) or another European Economic Area (EEA) competent authority and operating in the UK. They are also especially intended to apply to businesses making use of the grace period afforded to those that were providing AIS or PIS before 12 January 2016 (pre-January 2016 firms) which have not yet registered/authorised (see next for further detail).

[1] Some EU Member States are still in the process of transposing PSD2; in this case, more information can be found in the EBA's opinion on the transition from PSD1 to PSD2 here.

- These guidelines focus on organisations' interactions around credential sharing and as above refer to both regulated firms and grace period businesses. Accordingly, in these guidelines references to AISPs or PISPs cover all organisations offering these services, whether regulated firms or grace period businesses, unless otherwise specified, and references to "firms" includes both ASPSPs and AISPs and PISPs.
- For awareness: A regulated/authorised AISP or PISP should be included on the FCA's Financial Services Register or the public register of another EEA competent authority.
- Firms may also be on the Open Banking Directory (though not all firms will be reflected on the OB Directory[2]). The Directory is not an official national competent authority register.
- Businesses providing AIS or PIS before 12 January 2016 are able to continue to operate without registration/authorisation before the RTS comes into force. These businesses are often referred to as "pre-January 2016 firms" or those benefitting from the "grace period", and in these guidelines, we have referred to them as the "pre-January 2016 firms". Grace period businesses are subject to the same general data privacy and data protection laws as regulated firms. As per Guideline 2 below a contacts list of pre-January 2016 firms will be made available, however the list is, by its nature, not an exhaustive list of all such firms making use of the grace period[3].
- Credit institutions do not need additional authorisation to be able to offer AIS or PIS: they are included on the FCA's Financial Services Register or the public register of another EEA competent authority as a credit institution. Electronic money institutions or payment institutions wishing to offer AIS or PIS will need to 'top-up' their permissions with the relevant regulator to offer AIS or PIS.

Whilst businesses operating in the market pre-January 2016 are able to make use of a grace period to continue to operate after 13 January 2018 for a limited time without registration/authorisation, we strongly encourage such businesses to apply for the appropriate registration/authorisation or permission as soon as possible. There are market benefits as well as legal and regulatory benefits from doing so.

We are of the strong view that the entire market can best achieve the aims and vision of 'open banking' and of PSD2 through the use of open, PSD2-compliant APIs (Application Programming Interfaces) as they provide access to payment accounts to authorised/registered entities.

Therefore, as far as possible in the transitional period, we would encourage firms to make use of Open Banking APIs (as they apply to current account products and subsequently widen their scope) or PSD2-compliant APIs that an ASPSP has exposed to the market, as long as these APIs offer an equivalent level of functionality and service to that provided for the customer through their online banking/mobile banking interface.

- There are some businesses that provide technical services on another organisation's behalf for AIS or PIS. These businesses may not always be, and are not required to be, regulated. These businesses are often termed Technical Service Providers (TSPs), and can also provide services to pre-January 2016 firms. A TSP provides the technology connection for third parties for functions such as credential sharing through to screen scraping.
- For further background information please refer to annex 1.

[2] Firms will need to become authorised and go through a separate enrolment process before being included on the Open Banking directory.
[3] Not all pre-January 2016 firms are known, as the firm could also be a firm passporting into the UK. Any firm not included in the FCA Financial Services Register or Open Banking Directory is encouraged to get in touch.

Guideline 1: Contact/ relationship prior to initiation of a request

- 1.1 Where a relationship is not already in place, we would encourage AISPs and PISPs to make general contact with an ASPSP at the earliest opportunity to begin to build a relationship in advance of initiating a data request/initiating a payment (where possible), despite this not being a legal requirement.
- 1.2 General contact in advance helps with market cooperation to ensure a smooth transition away from the use of screen scraping and towards collaborative and open APIs noting that most AISPs and PISPs will during the transitional period be using mixed methods of access (coupling use of an API and screen scraping). This may also extend to after the RTS come into force for accounts falling outside the scope of PSD2. Screen scraping without proper identification cannot be used to access online payment accounts once the RTS come into force. Market cooperation will help provide additional confidence to both parties and ensures more efficient resolution in the case of a dispute.
- 1.3 We would encourage all firms (AISPs, PISPs and ASPSPs) to have dedicated teams/ points of contact for engagement. ASPSPs should provide a clear and transparent communication point for AISPs/PISPs to be able to quickly resolve a query or challenge related to the blocking of access. In the event this is not possible, please refer to Guideline 4.
- 1.4 Sharing information like ranges of IP addresses used to initiate a service request – when feasible[4] – is helpful for AISPs/PISPs and the ASPSP to ensure that the ASPSP is aware they may receive a request to access customer accounts, and therefore don't mistakenly and unduly block the AISP/PISP. In the case of a four-party model (i.e. a regulated entity making use of a technical service provider to aggregate data) this will often reflect the TSP's IP addresses.
- 1.5 It is also beneficial to share information like 'trading as' names, as it is difficult for firms to always establish the authorisation status of firms with complex structures when checking competent authority registers.
- 1.6 Where ASPSPs have separate means of access (e.g. screen scraping with a specific form of identification, sometimes referred to as screen scraping +), these should be published on the ASPSP's website in a publicly and easily accessible way, so AISPs/ PISPs can access the information.
- 1.7 ASPSPs are bound by their legal obligations under PSD2 to provide access to AISPs and PISPs. AISPs and PISPs are encouraged to follow these guidelines in order to reduce the risk of unnecessary friction.
- 1.8 Where an AISP/PISP complies with these guidelines, the ASPSP should ensure pro-active cooperation for facilitating AIS/PIS access to their customers' accounts.

Guideline 2: Identification of AISPs/PISPs to ASPSPs

- 2.1 As far as possible, AISPs and PISPs should identify themselves towards the ASPSP when they are accessing customer accounts. There are a number of market accepted ways of doing so. As per Guideline 1, the format of communication is something that can be discussed with ASPSPs in advance of initiating a data request/initiating a payment.
- 2.2 While not being legally required to identify themselves before the RTS apply, AISPs and PISPs should be transparent and open about their identities when interacting with ASPSPs. This identification could happen in one of two ways – either to communicate as part of the request (where possible) or, in any event, to contact ASPSPs in advance of making any requests (see Guideline 1). EEA firms passporting into the UK are also encouraged to be open about their identities. The ASPSP will ensure access for that AISP/PISP to their customers' accounts, apart from when there are objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account as outlined under Article 68(5) of PSD2.
- 2.3 ASPSPs must not block the access – including via screen-scraping – by those firms falling under the scope of these guidelines, unless there are objectively justified and duly evidenced reasons relating to unauthorised or fraudulent access to the payment account, as outlined under Article 68(5) of PSD2.

[4] Giving a range of IP addresses could be difficult when hosted on a public cloud provider. In such cases, ASPSPs and PISP/AISPs should communicate on possible alternative means of identification.

- 2.4 All regulated firms are encouraged to enrol in the Open Banking Directory.
- 2.5 AISPs and PISPs are encouraged to make use of the certificates issued by the Open Banking Directory or other similar directory initiatives to cryptographically sign the HTTP requests they make on behalf of the customer. Such an approach can take place when access occurs via the customer interface and is sometimes referred to as "the live market solution". This would allow ASPSPs to securely verify the identity of the AISP/PISP should they wish to, and requires no active checking from an ASPSP perspective.
- 2.6 A contacts list of pre-January 2016 firms including companies, trading names and key contacts will be published in early June. This list will contain names of businesses relying upon the pre-12 January 2016 grace period (otherwise called pre-January 2016 firms). Any business making use of this grace period is encouraged to get in touch to ensure they are reflected on this list by the 31 May 2018. Please get in touch with FDATA here.

  Businesses (including pre-January 2016 firms) will be responsible for notifying FDATA of changes to the list and the maintenance of their own information on the list at all times, including ensuring contact details and information is up to date and relevant. UK Finance, the Electronic Money Association, the Financial Data and Technology Association and techUK accept no legal responsibility for the accuracy or completeness of any information contained in the list, nor any ongoing responsibility for maintaining or updating the list.

Guideline 3: Fraud prevention and mechanisms for intelligence sharing

- 3.1 All regulated firms – whether an ASPSP, AISP or PISP – are required to have in place policies and procedures to monitor, identify and prevent fraud in compliance with PSD2, local regulatory requirements, and various European Banking Authority (EBA) Guidelines for ongoing operation.
- 3.2 UK Finance and other trade or commercial entities provide mechanisms for fraud data and intelligence sharing between financial services institutions, law enforcement and other key stakeholders. The primary function of these services is to facilitate collaborative activity between industry participants and with other partners committed to fighting fraud. Firms can find further information on how to get involved by getting in touch with UK Finance or other commercial entities.
- 3.3 All firms, including ASPSPs, AISPs and PISPs should consider signing up to and promoting the industry's 'Take Five' anti-fraud messages campaign. Further information is available here.

Guideline 4: Dispute resolution

- 4.1 In the interests of treating complainants fairly all firms (even those still to become authorised) should have procedures in line (or seek to become in line) with the FCA's dispute resolution (DISP) rules, that apply to Payment Service Providers as far as they apply to AIS and PIS services.
- 4.2 The Financial Ombudsman Service (FOS) is the nominated ombudsman set up to resolve complaints between financial services providers and their consumer and micro-enterprise customers in the UK. Pre-January 2016 firms are outside of FOS jurisdiction. However, for situations where things go wrong cooperation between firms is encouraged, and contact prior to the initiation of a request will help to ensure firms have this relationship already in place.
- 4.3 To help resolve disputes that fall outside of the FOS jurisdiction, firms are encouraged to consider the use of suitable alternative dispute resolution schemes, including subscribing to the FOS voluntary jurisdiction. Commercial propositions that relate to APIs and to non-API routes of access are widely available and there are industry solutions operated by Open Banking (available here) and Preta (in development and will be announced in due course). As per Guideline 1, firms should be proactive in contacting other firms in advance of disputes arising.
- 4.4 All firms will be subject to data protection law in addition to the requirements of PSD2. If there are concerns about a breach of data protection law, firms should contact the Information Commissioner's Office (or another EU data protection regulator) here.

Guideline 5: Clarity to the customer around consent and communications

- 5.1 In the interest of the customer experience, duplicate consent by both ASPSP and AISP/PISP should be avoided where possible[5]. Therefore, unless they have reason to believe otherwise, ASPSPs should assume that any AISP or PISP wishing to access a customer's account on behalf of the customer has their consent and should accept presentment of accurate authentication credentials as evidence of such consent[6].
- 5.2 All firms, including ASPSPs, AISPs and PISPs are expected to be clear with customers at all times with regard to consent and how their data is handled. As far as possible, consent should be requested via plain, easy to understand language.
- 5.3 AISPs/PISPs should always capture consent for a customer opting to use their services and for which purpose they are doing so. This also means that AISPs/PISPs should ensure that there is a clear record and traceability of any consent in relation to data being requested or a payment being made.
- 5.4 All AISPs/PISPs are bound by their legal obligations under PSD2 to not request data or use, access or store data other than for the relevant activity of AIS or PIS, for which the customer has given their consent to ensure that activities are not unduly blocked by ASPSPs. Accordingly, AISPs/PISPs are encouraged to collect precise consent which can be demonstrated if a dispute arises.
- 5.5 All firms should work in a way that delivers access in the interest of the end customer, by improving security and facilitating innovation. All firms should ensure helpful communications to customers by providing balanced information about newly-regulated services available to them.
- 5.6 Responsibility for unauthorised transactions should not be placed on customers unless there is clear evidence to that effect. ASPSPs must not prohibit or discourage customers from using AISPs or PISPs by communicating or suggesting to customers that they may themselves be responsible for unauthorised transactions, in circumstances where they would not be liable[7].
- 5.7 Customers often change their passwords with their ASPSP without the knowledge that this will affect how they log into their AISP/PISP. Firms should contact ASPSPs if it is possible this is the reason why an AISP/PISP can no longer access a customer account.

Guideline 6: Personalised Security Credentials management

- 6.1 In the interests of customer protection, all firms (AISPs, PISPs and ASPSPs) should as far as possible abide by rules that protect the confidentiality and integrity of personalised security credentials (as outlined in Articles 65, 66 and 67 of PSD2 and Chapter IV, Articles 22 through 27 of the RTS, which will come into force on 14 September 2019). The final RTS can be found here.
- 6.2 These rules include requirements around the creation and transmission of credentials by firms, the delivery of credentials, authentication devices and software to the customer and their association with the payment service user. It also includes requirements around the destruction, deactivation and revocation of credentials and consent.
- 6.3 Firms should always ensure the confidentiality of personalised security credentials and these should only ever be used based on the consent of the customer. AISPs and PISPs must ensure that personalised security credentials are not accessible to other parties, with the exception of the user and the issuer.

[5] As per the FCA Approach Document paragraph 17.48: https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017.pdf

[6] As per FCA's Approach Document paragraph 17.48: "ASPSPs are not required to check the terms of the consent provided by the customer ..., nor are they able to seek proof, or confirmation from the customer, of that consent as a prerequisite to fulfilling their obligations to provided access ...".

[7] However, the guidelines acknowledge that responsibilities may be different for different types of customers (for example corporate customers).

Guideline 7: Use of APIs in advance of RTS requirements

- 7.1 The market can best achieve the aims of open banking and of PSD2 through the use of open, PSD2-compliant APIs (Application Programming Interfaces).
- 7.2 As far as possible in the transitional period we would encourage firms to make use of Open Banking APIs (as they apply to current account products and subsequently widen their scope) or PSD2-compliant APIs that an ASPSP has exposed to the market, as long as these APIs offer an equivalent level of functionality and service to that provided for the customer through their online banking interface.
- 7.3 ASPSPs may also be in the process of developing common PSD2-compliant APIs; we would encourage firms to work together on these APIs.

Guideline 8: Authorisation

- 8.1 Whilst there is a grace period given to pre-January 2016 firms, firms are encouraged to become registered or authorised as soon as possible. There are market benefits as well as legal and regulatory benefits from doing so.
- 8.2 Firms that are not yet registered or authorised will not benefit from most of the legal and regulatory protections under PSD2 (for example, giving the customer the legal right to make use of a registered/authorised AISP/PISP and requiring the customer's ASPSP to provide access which is not dependent on the existence of a contractual relationship).
- 8.3 ASPSPs should check the FCA Financial Services Register or the public register of the other EEA competent authorities (pending development of the EBA's own electronic, central register as envisaged under Article 15 of PSD2), to verify that AISPs/PISPs that have been contacting them are registered/authorised. Pre-January 2016 firms will particularly benefit from compliance with these guidelines.
- 8.4 Cooperation and communication between firms, whilst not legally mandated, is to be expected and encouraged, and firms should set out contact points in a clear and accessible manner.
- 8.5 As per Guideline 4 pre-January 2016 firms are encouraged to implement procedures that are in line with the FCA's dispute resolution (DISP) rules.

Annex 1: Further Information on market before PSD2

- Before PSD2 came into force, access to payment accounts by what are now commonly called AISPs and PISPs in the EU was not a regulated activity[8]. For awareness, AISP and PISP services before becoming regulated activities were facilitated by:
- Direct, commercial relationships between banks and third party firms.
- Customers storing online credentials in a local application on their own equipment and then using these to open accounts, before then relaying the data onto the third party.
- A third party process that has attracted various names over the years, often called screen scraping, credential sharing or data harvesting. This effectively means that the third party, often using a Technical Service Provider to perform the service, securely captures and – in some cases - stores an end customer's online banking login details and uses these credentials to access the account on behalf of the customer.
- 'Credential sharing' and 'screen scraping' are not the same thing, as it possible, for example, to use stored credentials to connect through an API or dedicated interface. Screen scraping refers particularly to the process of copying data displayed on a screen and recombining into another application.
- During the transition period, each of these methods will continue and will operate in parallel to any new API or API standards emerging, such as provided through the UK's Open Banking Implementation Entity (OBIE).

[8] Some EU Member States are still in the process of transposing PSD2; in this case, more information can be found in the EBA's opinion on the transition from PSD1 to PSD2 here