PSD2 – authorisation, re-authorisation and new permissions in a post-Brexit world

PSE Payments Gateway Conference

John Burns

Payment Services Director, Compliancy Services Ltd

23rd May 2017

Compliancy Services

Informing Action · Inspiring Confidence

PSD2 – UK Implementation

- Compliancy Services is a leading UK FCA compliance consultancy. We help financial services firms achieve authorisation, manage their regulatory obligations and empower their staff with focused compliance training.
- Our compliance consultants are subject-matter experts and assist clients from a broad range of areas.
- Our dedicated Payment Services Practice is led by John Burns who is one of the UK's leading compliance experts in payment services. John has previously worked at the Financial Services Authority (now the FCA) and at major banks. He helped draft and then implement the original Payment Services Regulations and E-Money Regulations.

PSD2 – UK Implementation

- Still planned to implement in full & on time
- SCA seen as basis for Open Banking project
- Re-authorisation of 400+ APIs & EMIs by July 2018
- FCA consulting on additional requirements for Small PIs & Small EMIs – Possibly another 1,000+ re-registrations
- General Election delays final answers further

Scope changes

- Changes to Commercial Agents exemption will bring a number of currently exempt businesses into scope and require authorisation/registration.

- Changes to Limited Network exemption will bring other currently exempt businesses into scope and require authorisation/registration, many others will require to notify and justify use of exemption.
- Possibly thousands of businesses affected – most completely unaware that they are even using the exemption.

Authorisation & Registration

- All existing Authorised Payment Institutions and E-Money Institutions will need to be “re-authorised”
- FCA consulting on whether new requirements for SPIs and SEMIs
- There will be a fee, but this is still to be decided.
- Additional requirements regarding procedures for security incidents, control of sensitive payment data & continuity arrangements.
- Additional requirement to specify at least annual offsite or onsite checks on agents & branches
- New AISP/PISP permissions and requirements for firms taking these up

New Authorisation Requirements (1)

- Article 5(1) - (f) a description of the procedure in place to monitor, handle and follow up a security incident and security related customer complaints, including an incidents reporting mechanism which takes account of the notification obligations of the payment institution laid down in Article 96
- Article 96 sets out obligations on all PSPs to report “major operational or security incidents” to the competent authority
- The EBA is consulting on what constitutes a “major incident”- see website
- All PSPs (not just APIs & EMIs) will need to develop these procedures, and APIs & EMIs will need to submit these to the FCA for approval to retain authorisation.

EBA Draft Guidelines on Article 5(1)(f)

Guideline 9: Procedure to monitor, handle and follow up on security incidents and security-related customer complaints

9.1. The applicant should provide a description of the procedure in place to monitor, handle and follow up on security incidents and security-related customer complaints to be provided by the applicant, which should contain:

a) the individual(s) and bodies responsible for assisting customers in case of fraud, technical issues, and/or claim management;

b) the contact point for customers, including name and email address;

c) the procedures for the reporting of incidents, including the communication of these reports to internal or external bodies, including notification of mayor incidents to NCAs under Article 96 of PSD2 and in line with the EBA Guidelines on incident reporting (EBA/GL/2016/tbc); and

d) the monitoring tools used and the follow-up measures and procedures in place to mitigate security risks

EBA Draft Guidelines on Article 5(1)(g)

Guideline 10: Process to file, monitor, track and restrict access to sensitive payment data

10.1. The applicant should provide a description of the process in place to file, monitor, track, and restrict access to sensitive payment data consisting of:

a) a list of the data classified as sensitive payment data in the context of the payment institution's business model;

b) the procedures in place to authorise access to the sensitive payment data;

c) a description of the monitoring tool;

d) the access right policy, detailing access to all relevant infrastructure components and systems, including data bases and back-up infrastructures;

e) unless the applicant intends to provide PIS only, a description of how the collected data is registered;

EBA Draft Guidelines on Article 5(1)(g)

f) unless the applicant intends to provide PIS only, the expected internal and/or external use of the collected data, including by counterparties;

g) the IT system and technical security measures that have been implanted, including encryption and/or tokenization;

h) identification of the individual(s), bodies and/or committees with access to the sensitive payment data;

i) an explanation of how breaches will be detected and addressed; and

j) an annual internal control program in relation to the safety of the IT systems.

New Authorisation Requirements (2)

- Article 5(1) - (g) a description of the process in place to file, monitor, track and restrict access to “sensitive payment data”
- Note definition of “sensitive payment data”:
  - “data, including personalised security credentials which can be used to carry out fraud. For the activities of payment initiation service providers and account information service providers, the name of the account owner and the account number do not constitute sensitive payment data”
- All APIs & EMIs will need to identify what data meeting this definition they hold, develop processes and procedures and submit these to the competent authority for approval to retain authorisation

New Authorisation Requirements (3)

- Article 5(1) - (h) a description of business continuity arrangements including a clear identification of the critical operations, effective contingency plans and a procedure to regularly test and review the adequacy and efficiency of such plans
- APIs & EMIs will need to identify their “critical operations” (including those outsourced) and submit their contingency plans to the FCA for approval to retain authorisation
- a description of the principles and definitions applied for the collection of statistical data on performance, transactions and fraud
- APIs & EMIs who are not currently collecting statistical data on these, will need to put processes in place to do so and submit these to the FCA

New Authorisation Requirements (4)

- Article 5(1) - (j) a security policy document, including a detailed risk assessment in relation to its payment services and a description of security control and mitigation measures taken to adequately protect payment service users against the risks identified, including fraud and illegal use of sensitive and personal data
- The security control and mitigation measures referred to in point (j) of the first subparagraph shall indicate how they ensure a high level of technical security and data protection, including for the software and IT systems used by the applicant or the undertakings to which it outsources the whole or part of its operations. Those measures shall also include the security measures laid down in Article 95(1). Those measures shall take into account EBA's guidelines on security measures as referred to in Article 95(3) when in place
- Article 95(1) - Member States shall ensure that payment service providers establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks, relating to the payment services they provide. As part of that framework, payment service providers shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents.

EBA Draft Guidelines on Article 5(1)(j)

Guideline 13: Security policy document

13.1. The applicant should provide a security policy document containing the following information:

a) A detailed risk assessment of the payment service(s) the applicant intends to provide, which should include risks of fraud and the security control and mitigation measures taken to adequately protect payment service users against the risks identified.

b) A description of the IT systems, which should include:

- i. the architecture of the systems and their network elements;
- ii. the business IT systems supporting the business activities provided, such as the applicant's website, wallets, the payment engine, the risk and fraud management engine and customer accounting;
- iii. the support IT systems used for the organisation and administration of the applicant, such as accounting, legal reporting systems, staff management, customer relationship management, e-mail servers and internal file servers; and
- iv. information on whether those systems are already used by the applicant or its group, and the estimated date of implementation, if applicable.

EBA Draft Guidelines on Article 5(1)(j)

c) An exhaustive list of authorised connections from outside with partners, service providers, entities of the group and employees of the applicant working remotely, including the rationale for such connection;

d) For each of the connections listed under point c), the logical security measures and mechanisms in place, specifying the control the applicant will have over these accesses as well as the nature and frequency of each control, such as technical versus organizational, preventive vs detective; real-time monitoring vs regular reviews, such as the use of an Active Directory separate from the group, the opening/closing of communication lines, security equipment configuration, generation of keys or client authentication certificates, system monitoring, authentication, confidentiality of communication, intrusion detection, antivirus and logs;

e) The logical security measures and mechanisms that govern the internal access to IT systems, which should include:

- i. the technical and organisational nature and frequency of each measure, such as whether it is preventive or detective or whether or not it is carried out in real time; and
- ii. how the issue of client environment segregation is dealt with in cases where the applicant's IT resources are shared.

f) The physical security measures and mechanisms of the premises and the data centre of the applicant, such as access controls and environmental security;

EBA Draft Guidelines on Article 5(1)(j)

g) The security of the payment processes, which should include:

- i. the customer authentication procedure used for both, consultative and transactional accesses, and for all underlying payment instruments;
- ii. an explanations on how the safe delivery to the legitimate payment services user and the integrity of authentication factors such as hardware tokens and mobile application is ensured, at the time of both, initial enrolment time and renewal; and
- iii. a description of the systems and procedures that the applicant has in place for transaction analysis and identification of suspicious or unusual transactions.
- h) a detailed risk assessment in relation to its payment services, including fraud and with a link to the control and mitigations explained in the application file, demonstrating that the risks are addressed;
- i) a list of the main written procedures in relation to the applicant's IT systems or, for procedures that have not yet been formalized, an estimated date for their finalisation; and
- j) any other information relevant to the risks arising from the specific activities of the applicant.

Operational & Security Risks (Art 95)

- Requirements for all PSPs (not just Payment Institutions) to establish framework… …to manage operational and security risks relating to the payment services they provide. To include incident management procedures
- At least annual assessment of risks and adequacy of mitigation measures and control mechanisms to be provided to the FCA

Incident Reporting (Art 96)

- Definition of “major” operational or security incident – Guidelines to be developed by the EBA
- Obligation to notify competent authority – details to be provided to EBA & ECB for possible onward transmission to other competent authorities (and Eurosystem) if warranted
- Obligation to inform customers if incident “has or may have impact” on their financial interests
- Annual statistical return by PSPs to the FCA on fraud relating to different means of payment. PSPs will need to start collating data

AISP & PISP Authorisation

- PISPs - Article 5(2) - applicants for PISP permissions must hold professional indemnity insurance, covering territories in which they offer services, or some other comparable guarantee against liability for claims from customers and/or other PSPs
- PISPs - Article 7(b) - PISPs must have initial capital of at least €50,000
- AISPs - Article 5(3) - Member States shall require undertakings that apply for registration to provide payment services as referred to in point (8) of Annex I, as a condition of their registration, to hold a professional indemnity insurance covering the territories in which they offer services, or some other comparable guarantee against their liability vis-à-vis the account servicing payment service provider or the payment service user resulting from non-authorised or fraudulent access to or non-authorised or fraudulent use of payment account information
- There is no capital requirement for AISPs

Passporting (1)

- All statements regarding passporting are, of course, subject to revision when the terms of Brexit become clearer
- Article 28 - new listing of information to be provided by applicant for passporting. Specific noting of AML/CTF as issues to be addressed
- This still seems to leave room for disputes between competent authorities
- 3 month time limit to notify competent authorities of host Member State
- Payment institution to notify home state Competent Authority of start date, Home State Competent authority then to notify Host State
- New obligations on payment institutions to advise Home State competent authority of changes
- EBA to develop technical standards.

Passporting (2)

- Article 29 - new provision taking in parts of old 25(3) & (4) on how passported agents and branches are to be supervised. New power for Host Member State to require passported payment institutions to report to them periodically. Also Host Member States may require passported payment institutions under right of establishment to appoint a central contact point in their territory. The nature of such a contact point will be critical in the impact on passporting firms

Passporting (3)

- Article 30 - measures in case of non-compliance, including precautionary measures
- Obligation on home state competent authority to act ‘without undue delay’ to make passporting PI comply when notified by Host State competent authority
- Power also in ‘emergency situations’ for Host State competent authority to take ‘precautionary measures’
- This potentially provides a “nuclear option” for some Member State competent authorities to stop a passported PI or EMI from operating. The Commission and the EBA have to be advised “without undue delay” which may help to avoid its misuse

BREXIT – What will it mean? (other than "Brexit")

Possible outcomes

- Transitional Period
- Equivalence
- “Hard Brexit”

Transitional period

- As we are for a period (3 years?) allowing continuing passporting etc.
- EBA RTSs still in effect
- More time to adapt

Equivalence

- EEA recognition that UK has equivalent legislation
- Should allow passporting to continue
- Possible issue around EBA role and its being subject to the ECJ
- Likely to become more difficult as time goes on and regulation diverges.

"Hard Brexit"

- Passporting ends on March 2019
- Need for UK firms to set up entity in EEA to take advantage of passporting
  - Where?
  - What functions can still be carried out in UK?
- EEA firms passporting into UK will need to set up UK entity and seek authorisation.
  - What functions can still be carried out in home state?

Summary

- UK implementation of PSD2 will happen
- Major challenges for FCA's Authorisations Department (not helped by election)
- Firms needing authorisation/reauthorisation need to begin preparing
- Brexit uncertainty, but action will be needed by firms whatever the outcome.

Specific questions or support

John Burns
Payment Services Director
Compliancy Services Ltd

Email: john.burns@compliancy-services.co.uk

Telephone: 020 3457 3173