Waiting for PSD2

Will the EU Digital Single Market deliver both payment security and access to information?

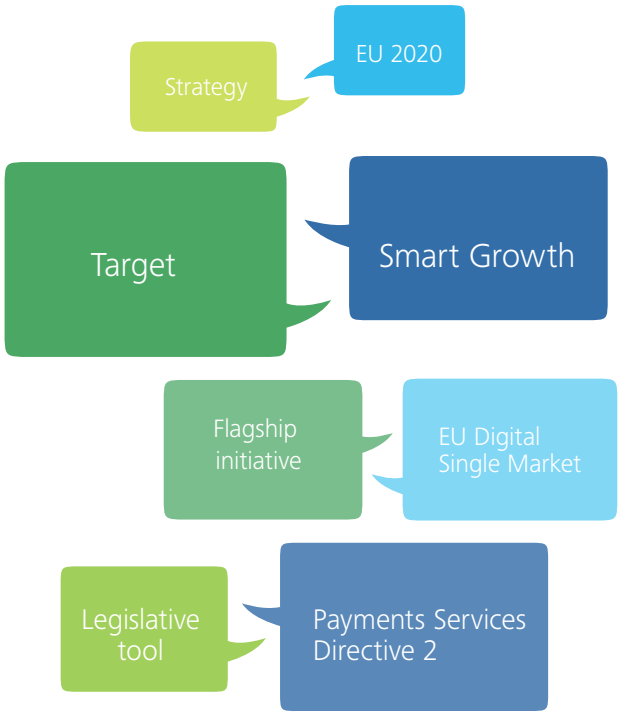
Pascal Martino
Partner
Strategy, Regulatory
& Corporate Finance
Deloitte

Charles Delancray
Director
Technology & Enterprise
Application
Deloitte

Giulia Bruni Roccia
Analyst
Operations, Excellence
& Human Capital
Deloitte

When Jean-Claude Juncker was nominated president of the European Commission (EC), he drew up an agenda for the work to be conducted by the EC between 2014 and 2019. The agenda comprised ten priorities, one of which being the achievement of "A Connected Digital Single Market"[1]. This priority is probably better known to the public as the flagship initiative "EU Digital Single Market"[2], one of three flagship initiatives proposed to achieve the smart growth target of EU 2020[3].

Figure 1: PSD2 and EU 2020



1 *European Commission, 2015. The Commissioners: Jean-Claude Juncker. Available at: http://ec.europa.eu/commission/2014-2019/president_en*

2 *European Commission, 2015. Digital Agenda for Europe, a Europe 2020 initiative: Digital Single Market. Available at: http://ec.europa.eu/digital-agenda/en/digital-single-market*

3 *The other two EU 2020 targets being "inclusive growth" and "sustainable growth". European Commission, 2012. Europe 2020: Flagship Initiatives. Available at: http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/flagship-initiatives/index_en.htm*

Essential for the development of the EU Digital Single Market is the legislation of the payment services market, a market regulated until today by *Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC,* referred to as the Payment Services Directive (PSD1)[4].

This directive is now in the process of being updated, as the Council of the EU (the Council), the European Parliament (EP) and the EC are negotiating to finalize the *Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC* (PSD2)[5]. PSD2 will bring some significant changes to the payment services market in order to align the EU with the inevitable and fast-moving technological changes currently underway.

We provide a brief summary of what these changes are, list the objectives they aim to achieve, and present the main players, both the actors who will be subject to and the stakeholders involved in the shaping of PSD2. We then focus on two specific aspects of the directive, namely payment security and access to information, and particularly on their potential incompatibility. Finally, we see how some stakeholders' initiatives could resolve this apparent incompatibility.

As the EU institutions are still at negotiation phase, and a solid analysis would have to wait until finalization of the directive and transposition of PSD2 into national laws, the goal here is merely to ask questions, raise doubts, and provide a taste for what could currently be missing in PSD2. So while we wait for PSD2 to be finalized, let us imagine we are part of the negotiation team and challenge each other with some points of view.

What is PSD2?

PSD1 has been in place since November 2007. Since then, the payment services market has undergone significant changes that require the EU legislation to be updated. When finalized, PSD2 will change both the territorial scope of the payment activities to be regulated, applying to transactions in non-EU currency where the Payment Service Provider (PSP) operating at both ends (payer and payee) is in the EU, as well as to all "one-leg transactions", i.e., transactions in all currencies where only one end's PSP is located in the EU. The currency scope is modified as well, as PSD2 transparency and information requirements will apply to transactions in any currency, and the provisions on rights and obligations in relation to payment service will apply to transactions in euro or in the currency of the Member State that is outside the euro area[6]. The negative scope changes, specifically in terms of commercial agents, limited network, telecom and ATMs. Notably, ATMs will be deleted from the list of exemptions, in order to contrast the growth

4 *Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32007L0064*

5 *Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547*

6 *Title 1, Article 2. Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547*

The EU institutions have embarked on a complex mission, as they aim to align the EU and national legislations with the ever-increasing number and variety of actors and activities of the payment services industry

of independent ATMs charging high fees for cash withdrawals[7]. All actors included in the scope will have to comply with specific changes in the provisions concerning transparency, security, liability, and consumer protection—including charges, fees, refunds, and complaints management.

Ultimately, PSD2 aims to:

- Further integrate payment services across national borders, strengthening the Single Euro Payments Area (SEPA) project
- In order to do this, ensure that the legislative framework is correctly applied by the regulatory authorities of each Member State, thus achieving standardization and interoperability of payment services, allowing them to become more secure and convenient, and digital and easier-to use
- Include more actors within the regulatory scope, thereby incentivizing a race for innovation, and increasing competition and the number of options available for consumers
- Enhance consumer protection

Clearly, this is not a simple task. The EU institutions have embarked on a complex mission, as they aim to align the EU and national legislations with the ever-increasing number and variety of actors and activities of the payment services industry. Ultimately, the EU institutions are aligning themselves with us. We are the consumers, and we are the ones who, for a while now, have clearly ceased to rely on the traditional bank alone; it is our transactions that now travel through a variety of not-so-traditional means. But do we know who these new actors are? Do we know about all the services available on the market?

7 *Explanatory Memorandum, Point 5. Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547*

Figure 2: PSD2 provides the following definitions

	Definition
Payment Service Provider (PSP)	A body providing: • "Services enabling cash to be placed on" or withdrawn from "a payment account as well as all the operations required for operating a payment account" • "Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider" and "execution of payment transactions where the funds are covered by a credit line for a payment service user." Both include "direct debits, including one-off direct debits; payment transactions through a payment card or a similar device; credit transfers, including standing orders" • "Issuance of payment instruments and/or acquisition of payment transactions" • "Money remittance" • "Services based on access to payment accounts provided by a payment service provider who is not the account servicing payment provider, in the form of payment initiation services, and account information services"
Account Servicing Payment Service Provider (ASP SP)	"A payment service provider providing and maintaining payment accounts for a payer."
Third Party Payment Service Provider (TPP SP)	"A payment service provider who is not the account servicing payment service provider" and provides "payment initiation services and account information services."
Payment Service User (PSU)	"A natural or legal person making use of a payment service in the capacity of either payer or payee."
Payment initiation service	"A payment service enabling access to a payment account provided by a third party payment service provider, where the payer can be actively involved in the payment initiation or the third party payment service provider's software, or where payment instruments can be used by the payer or the payee to transmit the payer's credentials to the account servicing payment service provider."
Account information service	"Payment service where consolidated and user-friendly information is provided to a payment service user on one or several payment accounts held by the payment service user with one or several account servicing payment service providers."

As is the case of all EU directives, proposals are discussed and negotiated between the EC, the EP, and the Council. These three institutions are now at the trialogue stage of negotiating the directive, and, according to the European Payments Council, EP approval of PSD2 is expected in September 2015, with publication in the Official Journal of the EU sometime during the winter. Member States will then have two years to transpose the directive into national legislation[8].

In addition to the three institutions, given the topic of PSD2, other EU stakeholders are called to provide recommendations and suggestions for amendments: this is the case of the European Central Bank (ECB) and the European Banking Authority (EBA). The latter, specifically, is responsible for designing the security guidelines to be applied by national regulators and all relevant actors in accordance with the PSD2[9]. The ECB and EBA are particularly relevant for the topic under discussion, as together they chair the European Forum on the Security of Retail Payments (SecuRe Pay Forum), a platform for the EBA and the members of the European System of Central Banks to develop common knowledge on security of payments[10].

Provisions on payment security and access to information

In order to provide consumers with convenient and easy-to-use services within a crowded and complex market, PSD2 aims to ensure the efficient and regulated exchange of information between the relevant actors. At the same time, consumers need to be reassured that this flow of information—as well as the payment services market in general—is secure.

"In recent years, the security risks related to electronic payments have increased, which is due to the greater technical complexity of electronic payments, the continuously growing volumes of electronic payments worldwide and the emerging types of payment services. As safe and secure payment services constitute a vital condition for a well-functioning payment service market, users of payment services should be adequately protected against such risks[11]."

PSD2 often merges the provisions for payment security and access to information in the same articles, as if to say that they inherently feed into each other, one being the essence of the other. But is it really so easy to assume that these two elements can fit together in the same legislation? Are they really that compatible? Let us have a look at what PSD2 legislates and we may see how the two could potentially be at odds.

In order to provide for payment security, PSD2 introduces the concept of "authentication" and "strong customer authentication". Authentication indicates *"a procedure which allows the payment service provider to verify the identity of a user of a specific payment instrument, including the use of its personalized security features or the checking of personalized identity documents[12]."* Strong customer authentication is different in that it is *"a procedure for the validation of the identification of a natural or legal person based on the use of two or more elements categorized as knowledge, possession and inherence that are independent, in that the breach of one does not compromise the reliability of the others and is designed in such a way as to protect the confidentiality of the authentication data[13]."*

8 *Boudewijn, G., 2015. PSD2: Almost Final – A State of Play. European Payments Council, 18 June 2015. Available at: http://www.europeanpaymentscouncil.eu/index.cfm/blog/psd2-almost-final-a-state-of-play/*

9 *Recital 80, Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547*

10 *European Central Bank, 2014. Mandate of the European Forum on the Security of Retail Payments. Available at: https://www.ecb.europa.eu/pub/pdf/other/mandateeuropeanforumsecurityretailpayments201410.en.pdf p.1 and p.2*

11 *Recital 6, Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547*

12 *Article 4, Clause 21, Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547*

13 *Article 4, Clause 22, Proposal for a Directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52013PC0547*

In order to provide consumers with convenient and easy-to-use services within a crowded and complex market, PSD2 aims to ensure the efficient and regulated exchange of information between the relevant actors

Article 87 legislates that PSPs apply strong customer authentication whenever the payer, or a TPP SP on behalf of the payer, initiates an electronic payment transaction. In the latter case, the ASP SP should then allow the TPP SP *"to rely on the authentication methods of the former when acting on behalf of the PSU"*. Furthermore, a TPP SP "shall authenticate itself towards the account servicing payment service provider of the account owner".

Article 62 also says that the PSP issuing a transaction should "make sure that the personalized security features of the payment instrument are not accessible to parties other than the payment service user entitled to use the payment instrument". It also establishes that the PSP will then bear "the risk of sending a payment instrument to the payer or for sending any personalized security features of it".

Article 58 should also be noted as it legislates on the access to and use of payment account information by TPP SPs:

"Where a third party payment service provider has been authorized by the payment service user to provide payment services, it shall have the following obligations:

1. To ensure that the personalized security features of the payment service user are not accessible to other parties
2. To authenticate itself in an unequivocal manner towards the account servicing payment service provider(s) of the account owner
3. Not to store sensitive payment data or personalized security credentials of the payment service user"

Provisions on payment security and access to information: a difficult coexistence

When looking at PSD2's approach to payment security and access to information, three main problems seem to arise, three sources of doubts that could be particularly important for the regulator, the consumer, or the relevant PSPs, depending on the case.

1

It is clear enough from a reading of PSD2 that the flow of information is vital for the processing of payments, and because so many different players are active in the same field, access to information needs to happen in a secure, authorized, and authenticated way. But exactly because so many different actors are involved, because the traditional, "old-fashioned", and "technologically-behind" actors (banks) are expected to work together with more innovative actors (such as the new emerging TPP SPs), the IT platforms used to share information may vary a lot. In some cases, these platforms have to be built from scratch, while others are already very sophisticated. This leads to a not-so-irrelevant hole in the process flow. A survey conducted by Finextra and FIS reveals exactly this gap:
"One risk of opening up access to data and functionality hosted in a bank's core system is that if the core systems are ancient and inflexible, these limitations become apparent outside the confines of the bank's operations teams. A greater risk is that this access can't be granted at all in a robust, secure manner due to these limitations[14]*."*

- This is relevant for: the regulator, who has to ensure that all actors have a standardized and interoperable platform; and all PSPs, even the most technologically advanced ones, who may suffer from having to "slow down" and adapt

2 to the pace of the less innovative ones

We have an understanding now of just how many authorizations are needed to access information and process payments, all very relevant steps to ensure security. But individuals (consumers, regulators, and PSPs) risk getting lost along the way, mistakes could be made at any point, and may go unnoticed as well.

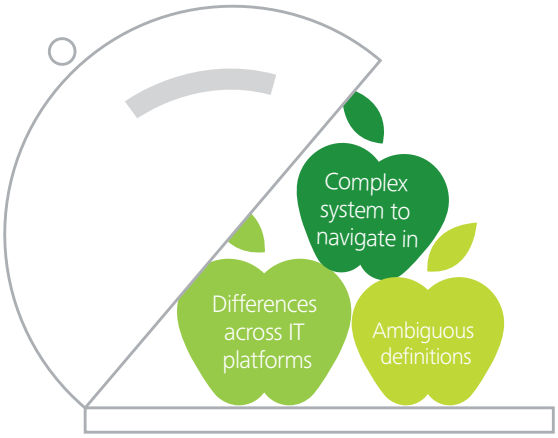
- This is relevant for: consumers, who, when encountering an incident may be unable to spot the wrongdoing, and unable to avail of the complaints-management possibilities offered by PSD2 (Articles 88-91). PSPs are also affected, as they need to make sure their process flow is very well oiled and aligned with other PSPs' process flow. It is also relevant for regulators, who have to oversee this alignment and interoperability

3

But even with all these authorizations to be granted in terms of access to information; even with the new authentication and strong customer authentication requirements; even with the warnings on who is liable in case the wrong information is shared with an unauthorized actor (Articles 79-83)—some elements remain blurry. Who defines what the "entitlement" to use a payment instrument is (Article 62)? What does it mean to "store" sensitive payment data (Article 58)? At what point of the payment process does the TPP SP have to get rid of this sensitive payment data in order to reassure the customer that the data has not been "stored" and is not being misused? The definition of what "authentication" means indicates that it is the procedure that allows the TPP SP to identify the payment user and "use" its credentials (Article 4). What activities fall under the verb "use"? Does it only include the pure transfer of credentials, the mere input of the credentials in order to authorize and process the payment? If so, it is not clear enough, and for all we know it could also include the activity of "storing"—which is forbidden according to Article 58.

- This is relevant for: the regulator, who will have to oversee the transposition of the directive into national legislation and is expected to be sure beyond doubt of what each term means, leaving no room for misunderstanding

Figure 3



Ensuring coexistence between payment security and access to information

The healthy development of any EU directive relies on the exchange of opinions, recommendations, and amendments, as each stakeholder tackles the topic in a different way. It is particularly interesting to look at the ECB and EBA positions, as they have quite heavily focused on the aspect of security. By looking at their opinions and recommendations, we may see ways of ensuring compatibility between payment security and access to information.

In January 2013, the ECB drew up the Recommendations for the Security of Internet Payments (ECB Recommendations). Later in February 2014, the ECB formed its opinion on the proposed legislation (ECB Opinion), focusing once again on the security issues (not yet) tackled by PSD2 and suggesting a list of amendments.

14 *Finextra, 2015. PSD2 and XS2A – Regulation or Opportunity? Report on a Survey by Finextra and FIS. Available at: http://www.fisglobal.com/ucmprdpub/groups/public_searchable/documents/webasset/c038915.pdf p.23*

The rationale of both documents is similar to that of the directive: flow of information is essential, but should be processed according to specific authorization and authentication steps. However, the ECB Recommendations and the ECB Opinion successfully avoid the gaps spotted in PSD2.

1. The problem of having non-standardized IT platforms does not arise, as the ECB Recommendations propose the best practice of PSPs *"using a single strong customer authentication tool for all internet payment services"* as *"this could increase acceptance of the solution among customers and facilitate proper use*[15]*."* Strong customer authentication should be fitted into *"a standardized European interface for payment account access*[16]*."* Admittedly this does require more work and legislation, but implementing one single strong customer authentication tool for all services ensures standardization, interoperability, and less room for doubt and/or mistakes. The good news is that the EU also has the means of instituting and implementing a single tool, through the EBA and even the SecuRe Pay Forum.

2. The ECB proposal for consumer awareness and education programs is very interesting. Such programs would solve the second problem of the lack of a good understanding of the authentication and authorization processes in the payments services market. Legislation regulating payment security and access to information is all well and good; but if the consumer is not actually aware of where the security threats lie, how to counteract them, and what kind of information about him/her is allowed to flow through the system, then he/she remains an unprotected consumer and the legislation is merely dry sterile soil. According to the ECB, the PSP could provide one secure communication channel through which to explain how the consumer can report suspicions on fraudulent activities, how the PSP will respond to complaints and enquiries, and how the PSP will notify the customer in case of its own suspicions[17]. Additionally, PSPs could provide customer education and awareness programs in order for the consumer to mature its knowledge of data protection and data management through all various devices (computers, phones, etc.), and the use of the *"genuine internet payment website of the PSP*[18]*."*

3. Finally, the ECB is also more precise in its definitions, as the ECB Opinion amendment for Article 58 shows. The interdiction to "store sensitive payment data of the payment service user" is further specified: *"…obtained when accessing the payment service users payment account, apart from information for identifying a payment initiated by the third party payment service provider such as the reference number, payer's and payee's IBAN, the transaction amount, other reference information and the settlement system information, and not use any data for other purposes than explicitly requested by the payment service user*[19]*."*

15 *European Central Bank, 2013. Recommendations for the Security of Internet Payments: Final Version After Public Consultation. Available at: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafter pc201301en.pdf p.10*

16 *Point 2.7, Opinion of the European Central Bank of 5 February 2014 on a proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65&EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Available at: https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2014_09_f_sign.pdf*

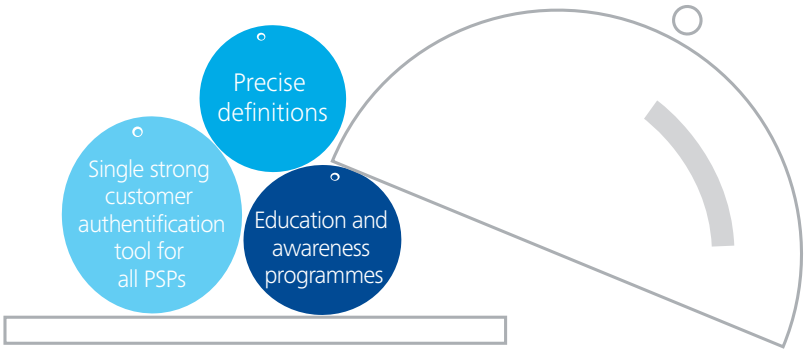
17 *European Central Bank, 2013. Recommendations for the Security of Internet Payments: Final Version After Public Consultation. Available at: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversion afterpc201301en.pdf p.13*

18 *European Central Bank, 2013. Recommendations for the Security of Internet Payments: Final Version After Public Consultation. Available at: https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafter pc201301en.pdf p.13*

19 *Amendment 24, Opinion of the European Central Bank of 5 February 2014 on a proposal for a directive of the European Parliament and of the Council on payment services in the internal market and amending Directives 2002/65&EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC. Available at: https://www.ecb.europa.eu/ecb/legal/pdf/en_con_2014_09_f_sign.pdf*

The ECB Recommendations were used by the EBA to draw its Guidelines on the Security of Internet Payments (Guidelines) in December 2014 and are valid as of August 2015. As a matter of fact, the EBA is a particularly important stakeholder: based on PSD2, it has the responsibility to design the security guidelines and define the technical standards that Member States should apply in line with the directive's changes in scope and requirements[20]. The Guidelines serve as preparatory work and only set "minimum security requirements for payment service providers across the EU"[21]. Unfortunately, however, even at this preparatory stage, implementation problems arise, as 3 out of 28 countries have already stated their inability (or potential unwillingness) to comply with the Guidelines[22].

Figure 4



Conclusion

Ultimately, we see that EU stakeholders are aware of the importance of payment security and access to information (refer to the responsibility assigned to the EBA by PSD2); we see that at least some of these stakeholders acknowledge the difficult coexistence and compatibility between payment security and access to information; and from these stakeholders we see concrete proposals for solutions (ECB Opinion and EBA/ECB proposals for best practices). However, will these solutions be included in the latest version of the directive? And how will they ultimately be transposed into national legislations, given the reluctance already expressed by some Member States to comply with the Guidelines?

We shall wait until the end of the year to see what happens at EU level, and check again in two years' time for the status at Member State-level. But one thing is sure—with PSD2, the EU really has the tangible chance of creating an EU Digital Single Market if loopholes are acknowledged and concretely resolved.

20 Directive, Recital 80; Article 86, Article 87

21 http://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

22 Namely, Estonia, Slovakia, and the UK.
European Banking Authority, 2015. Compliance Table – Guidelines. Available at: https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+Compliance+Table-GL+security+of+internet+payments.pdf