INTESA SANPAOLO
Transparency register 24037141789-48

June 2022

Targeted consultation on the review of the revised payment services directive (PSD2)

Intesa Sanpaolo Position Paper – focus on cybersecurity aspects

Intesa Sanpaolo, one of the top banking groups in Europe, welcomes the opportunity to contribute to the debate of the review of the revised Payment Services Directive (PSD2) and would like to complement its response to this consultation with further comments from a cybersecurity perspective.

Overall, the revised PSD2 **has positively contributed to both developing new technological solutions and increasing the safety in the payments market**. Notwithstanding, a "disproportion" in costs incurred for the implementation of the solutions, that are excessive when compared to the substantial benefits, should also be highlighted. Banks have invested resources to fight against phenomena external to the bank ecosystem but related, for example, to TELCOs or other external actors. Furthermore, an update of the Directive and its related technical RTSs is needed to keep up with the current technological developments.

Please, find below our key messages from a pure cybersecurity perspective:

- **Incident reporting harmonization**: an alignment between the PSD2 and other related regulations, including eIDAS, DORA, NIS2 and GDPR is needed with particular reference to the notification timeline. In our understanding, DORA seems to already meet this alignment with the PSD2 and we welcome this development;
- **The exclusion of TELCOs from the scope of the PSD2 appears unjustified**, especially considering that TELCO providers are increasingly part of the payment "chain" and, consequently, also involved in frauds. In addition, if the forthcoming European Digital ID Wallet (EDIW) will be used for payments authorization, also EDIW providers should fall under the scope of the PSD2;
- **E-money services** should be included in the scope of the Directive. We welcome the EBA proposal (*see its Opinion on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2)*) about the merger between the E-Money Directive (EMD2) and PSD2. Today, many e-money account holders may not be sufficiently informed about the difference between a bank account and an e-money account. In this regard, it is also necessary to ensure the protection of client's funds;
- Although the sanctions are proportionate and act as a deterrent, **PSD2 is currently not effective for all those transactions from EU to non-EU countries, and vice-versa**. These transactions could give rise to fraudulent actions since they are not clearly regulated;
- In terms of definitions, it is important to clarify at European level the concept of **payer negligence** (to reduce discretion at level of national legislation);
  We see a need to define the impact of PSD2 on the day-to-day experience of payment service users, especially in terms of **users' awareness of their rights and obligations** in relation to the **processes of recovering funds which are subject to fraud**. In addition, it could be important to achieve **a more balanced sharing of liabilities between ASPSPs and PISPs**, with

particular reference to **unauthorized payment transactions**. Given the fact that PISPs rely on the authentication procedures provided by ASPSPs to the payment service user, the burden of proof tends to fall mainly on ASPSPs. In addition, an ASPSP has an immediate compensation obligation and is entirely dependent on the solvency and availability of the PISP for receiving compensation. We believe that liabilities and risks in PSD2 are not equally balanced between ASPSPs and PISPs/AISPs and a review is therefore warranted. PSD2 requires ASPSPs to open their customers payment data to third parties and this could have repercussions regarding the security of customer financial data, risks of frauds and data breaches. Moreover, if the authentication method is provided by a third party (e.g. a digital wallet provider), its obligations and responsibilities should be defined as well;

- Regarding the interactions with TPPs, it would be appropriate to provide precise implementation standards for TPPs interfaces and authentication methods, in order to avoid that the implemented solutions are seen as obstacles by TPPs**;**
- The **peculiarity of communication protocols** that are **dedicated to corporates** must also be taken into account in the context of the possible revision of PSD2 since they are not offered to the consumers and have a different level of risk (especially with regard to the strict requirements defined for the **SCA**);
- **New attack models** used by fraudsters focusing on **human vulnerabilities** are also emerging (for example, exploiting **social engineering techniques**). A revision of "fraud" definition correlated to **payer manipulation** is therefore needed (in order to distinguish between phenomenology with a technical component and phenomenology based exclusively on social engineering attacks). **Faster and simpler procedures** are also needed **for recovering funds in the event of fraud;**
- Finally, to **combat cyber fraud**, we would like to suggest the following countermeasures:
  - the closure or suspension of potentially fraudulent websites should be centrally managed at the European level, in a quick and easy way. The removal of any web authentication certificates associated with the website, and more stringent verification requirements for requests to open websites, should be implemented. The bank's adoption of a .bank domain could also be considered, so that cyber criminals cannot open fraudulent sites;
  - structural strengthening of law enforcement at the European level and greater cooperation with financial institutions;
  - increased collaboration with TELCOs and establishment of suitable countermeasures to fight smishing. We suggest a sender verified ID register as a possible solution. This registry is designed to significantly reduce the impact of "smishing" and spoofing through fake SMS messages by criminals, helping to protect consumers and businesses alike. The registry contains the verified profile and phone number of the financial institution or company from which customers may receive informational SMS messages. We suggest combining the register of Alias with the register of numbers from which fraudulent SMS messages are sent;
  - public awareness campaigns and initiatives promoted at European level;
  - simplification of interbank rules and processes for blocking and returning fraudulently stolen funds;
  - development of a system, at European level, for verifying the beneficiary and consisting in a mechanism that allows the payer to verify the Payee's IBAN before performing the transaction. The so called "confirmation of payee" services (that check the payee's name provided by the payer against the actual account holder name associated on the systems of the Payee's PSP with the IBAN provided by the payer) and currently offered in some markets, could help to prevent frauds in certain scenarios. We suggest performing an impact assessment to verify in which cases and to what extent these services can help to prevent frauds, in order to quantify the benefits of a possible introduction and to determine the costs for the all banking system to implement and run such a mechanism. In addition, the development of a system for sharing IBANs involved in frauds at European

level (SEPA) is considered useful. More info sharing actions could, in fact, support fraud prevention;

- implement actions to prevent spoofing of the calling number, as well as on SMS messages and ensure the blocking of calls from toll-free numbers;
- solutions allowing to hinder the following phenomena: Caller ID spoofing, SIM Swap, unwanted and / or fraudulent calls.