29 April 2024

EBA-Op/2024/01

EBA Opinion on new types of payment fraud and possible mitigants

Executive summary

1. The EBA has recently assessed fraud data for the year 2022, which has become available at the end of 2023, arriving at insights on fraud patterns and new fraud types, including that instant payments feature notably higher fraud rates than traditional credit transfers, and that a relevant part of the fraud losses are borne by the customers, especially for credit transfers.

2. As to the emerging fraud types, the EBA observed that, while the mandatory application of Strong Customer Authentication (SCA) has been successful in preventing fraud based on the stealing of customers' credentials, fraudsters managed to adapt their techniques, giving rise to fraud types of a more complex nature, in particular leveraging on social engineering.

3. Based on the insights gained, the EBA arrived at the view that security measures are needed, in addition to those articulated in the EU Commission's proposals for a Third Payment Services Directive (PSD3) and a Payment Services Regulation (PSR) as well as the recently adopted Instant Payments Regulation, so as to address the dynamic nature of fraud observed. The Opinion on hand articulates recommendations for such additional measures, and they have benefited from recent fraud prevention experiences by national competent authorities (NCAs) in their jurisdiction.

4. The aim of this opinion is to help further strengthen the forthcoming legislative framework under PSD3 and PSR, which will enshrine anti-fraud requirements for retail payments for several years.

Introduction and legal basis

5. On 28 June 2023, the European Commission published its proposals for a revision of the existing Payment Services Directive (PSD2), in the form of a proposed PSD3 and a Payment Services Regulation (PSR).

6. The EBA welcomes that the proposals incorporate many of the 200+ recommendations that the EBA had addressed to the EU Commission in its Opinion of June 2022[1]. This was particular so for those recommendations that were aimed at further reducing payment fraud and enhancing the security of retail payments, which were themselves a result of the EBA's and NCAs' observations of how payment service providers (PSPs) had complied with the requirements set out in PSD2.

7. Since the publication of the EBA's Opinion of June 2022, the EBA has carried out further work to assess new fraud trends and types of payment fraud, leveraging on the new fraud data that became available to the EBA and the European Central Bank (ECB) at the end of 2023. This analysis was further informed by additional data collection conducted with NCAs in 2023 on particular data points that are not requested under the EBA Guidelines (GL) on fraud reporting under the PSD2[2], such as data on fraud for instant credit transfers and fraud related to the so-called mail orders or telephone orders (MOTOs). Moreover, the assessment of new fraud types draws on input provided by authorities responsible for the supervision of PSPs as well as those responsible for the oversight of payment systems and instruments, including the ECB.

8. Based on this assessment, the EBA arrived at the view that relevant insights can be gained, in particular regarding:

    a. The impact that the security requirements under PSD2 have had on fraud levels across the EU;

    b. Emerging fraud trends observed and new types of payment fraud;

    c. Potential additional measures to combat fraud, beyond the fraud mitigation measures proposed by the EU Commission in the PSD3 and PSR proposals and the service ensuring verification of the payee in case of credit transfers in Euro (also known as the IBAN/name-check) introduced in Regulation (EU) No 260/2012 (the SEPA Regulation) by Art. 1(2) of the Regulation (EU) 2024/886 on instant credit transfers in euro (the

[1] Opinion of the European Banking Authority on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2) – see https://www.eba.europa.eu/sites/default/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

[2] https://www.eba.europa.eu/sites/default/files/documents/10180/2281937/5653b876-90c9-476f-9f44-507f5f3e0a1e/Final%20report%20on%20Guidelines%20on%20fraud%20reporting%20under%20Article%2096%286%29%20PSD2%20%28EBA-GL-2018-05%29.pdf

"Instant Payments Regulation")[3] which was published in the Official Journal of the EU on 19 March 2024.

9. These insights are presented below in turn under "General comments", followed by possible additional measures for consideration by the EU co-legislators and the Commission, under "Specific proposals".

10. The figures and observations included in the next section of this Opinion are based on selected fraud data collected by the EBA and the ECB for 2022 under the EBA GL on fraud reporting under PSD2, except for the figures on MOTOs and instant payments (respectively, in paragraphs 15 and 17) that are based on a separate survey conducted by the EBA through the NCAs and national central banks in 2023, with H1 2022 as reference period.

11. The competence of the EBA to deliver this opinion is based on Art. 1(5) and Art. 16a(1) of Regulation (EU) No 1093/2010, as part of the EBA's objective to 'contribute to enhancing customer protection' and 'play an active role in building a common Union supervisory culture and consistent supervisory practices, as well as in ensuring uniform procedures and consistent approaches throughout the Union'.

[3] Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro

General comments

Impact of the security requirements under PSD2 on fraud levels across the EU

12. Based on the assessment of the payment fraud data collected under PSD2, the EBA has observed that SCA, complemented by transaction monitoring as well as the other security measures imposed by the PSD2 and the EBA Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication under PSD2 (the RTS)[4], has been successful in mitigating fraud overall.

13. For example, fraud levels for credit transfers have been contained to 0.0008% of the total value for credit transfers (i.e., 8 euro defrauded out of 1 million euros transmitted) and 0.0020% for direct debits in 2022. For card payments, while the absolute fraud rate is higher, i.e. 0.029% in value (according to data reported by payer's PSP), the average fraudulent transaction is limited to €80, compared to a corresponding value of €2,252 for credit transfers. Already in 2020 – 2021, in the period of migration to SCA, the EBA had observed a reduction in the average fraud rate in value between 40% and 60%, in card payments alone[5]. Similarly, more recently, the ECB card fraud statistics published in May 2023[6] show that the implementation of SCA by PSPs and merchants in 2021 was accompanied by a significant decline of remote card payments fraud.

14. In parallel, the EBA observes that SCA is now widely used to authenticate remote electronic transactions, including those for e-commerce. Indeed, while several exemptions to the use of SCA were provided in the RTS, with the aim of supporting user-friendly and innovative means of payment while taking into account the need to ensure the safety of customers' funds and personal data, in 2022 SCA was applied for 70% of remote credit transfers and 36% of remote card transactions (as reported by the payer's PSP), for a percentage of the aggregate value of 77% and 55% respectively. Correspondently, the use of the exemptions to SCA set out in the RTS has been generally limited for these two payment instruments. In particular, SCA exemptions were used for 32% of remote card transactions.

15. The EBA has also observed that PSPs have reported a high volume of non-SCA authenticated transactions as merchant-initiated transactions (MITs)[7], equivalent to 13.1% of all remote card-based payments in the EU (as reported by the payer's PSP) . Similarly, payment transactions by mail order or telephone order (so called MOTO transactions), which are out of scope of the SCA

[4]Commission Delegated Regulation (EU) 2018/389 - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0389

[5]See EBA Report on the data provided by PSPs on their readiness to apply strong customer authentication for e-commerce card-based payment transactions (https://www.eba.europa.eu/publications-and-media/press-releases/eba-publishes-report-data-provided-psps-their-readiness-apply)

[6] https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html

[7] MITs include card-based payments initiated by a payee, without any interaction or involvement of the payer, based on an agreement between the payer and the payee under which the payer authorizes the payee to initiate those transactions. The EBA Guidelines on fraud reporting under PSD2 stipulate that, for a transaction to qualify as an MIT and thus be considered as payee initiated and not subject to the requirement in Art. 97 PSD2 to apply SCA, it needs to meet the condition specified by the EU Commission in Q&As 2018 4131 and 2018 4031.

requirement, were significant in volume, too. Both MITs and MOTO transactions featured considerably higher fraud rates in H1 2022 (i.e. more than 0.1% in value – or more than 1 euro defrauded out of 1000 euros transmitted) both with respect to SCA authenticated transactions and transactions exempted from SCA.

Emerging fraud trends and new fraud types observed

16. Despite the positive effect SCA has had in terms of fraud reduction, discussed in paragraph 13 above, the EBA has observed high levels of fraud for some specific payment instruments, geographic dimensions, jurisdictions, or combinations thereof.

17. The first is instant credit transfers, also referred to as instant payments, for which the data reported by 18 NCAs for H1 2022, show that the fraud rates in value, besides presenting significant divergences between Member States (MS), are about 10 times higher on average than conventional Credit Transfers (CT).

18. The EBA considers that it is too early to clearly identify the root causes of these findings, and that account needs to be taken of recent observations in some MS that instant payments are less used by corporates than traditional credit transfers. Nevertheless, the EBA is of the view that the aforementioned higher fraud rate of instant payments may be partially due to the fact that the possibility for PSPs to recover funds in case of fraudulent instant payments is limited or non-existent, given that those payment are executed in less than 10 seconds - which may make instant payments more appealing to fraudsters. Relatedly, this finding may also be linked to the technical constraints associated with the application to instant payments of transaction monitoring and subsequent treatment of suspicious transactions by PSPs. The above highlights the need to ensure that there are appropriate security safeguards in place for instant payment transfers to mitigate the risk of fraud, particularly given that, with the application of the Instant Payments Regulation, it is expected that instant payments will be increasingly used by customers in the EU.

19. Second, the EBA observed that fraud rates for cross-border transactions are much higher than for domestic ones (i.e. transactions where the payer's PSP and the payee's PSP are located in the same MS), across all payment instruments included in the payment fraud reporting framework under the PSD2. This applies to both cross-border transactions among countries in the Economic European Area (EEA)and cross-border transactions between an EEA country and an extra-EEA country. For example, the EBA's analysis of the aggregate data at EEA level for 2022 suggests that, for both cards and credit transfers, cross-border fraud rates in volume are about 9 times higher than for domestic transactions. The observations of NCAs and views expressed by market operators suggested that this may be primarily due to insufficient cross-border cooperation among PSPs and other involved stakeholders to deal with criminal activities of an international nature, as well as, in the case of cross-border transactions involving extra-EEA countries (one-leg transactions), the uneven application of SCA.

20. Third, in practice, the distribution of liability for fraud losses in the EEA between the payment service user (PSU), on the one hand, and the PSP or other entities on the other, varies remarkably across payment instruments. For example, in 2022, while for card payments the losses are approximately equally split between PSUs and PSPs plus other entities, for credit transfers the share of losses borne by the PSU is 79%, which equates to €1.2B in absolute terms. The share of losses borne by the PSU also varies considerably across the EEA.

21. This finding could be partially explained by the fact than an increasing number of payment fraud takes the form of manipulation of the payer, or the so-called "Authorized Push Payment" fraud, where the payer is manipulated into making a payment to the fraudster. Furthermore, in the EBA's view, the lack of a clear delineation between authorized and unauthorized transactions in the PSD2, leading to divergent application of the relevant liability rules across MS, and the broad interpretation in some MS of the notion of "gross negligence" may also partially explain why a large percentage of losses in case of fraudulent credit transfers are borne by the PSU. In this regard, the EBA observed the practice by PSPs, common in some MS, to consider all SCA authenticated transactions as authorized, even in case of social engineering fraud, and to refuse reimbursement of customers in such cases, as they consider that the limitation of liability of the payer in Art. 74 PSD2 does not apply in such cases.

22. Moreover, the EBA observed that the fraud rates vary notably across EEA countries for all the payment instruments considered, with some MS featuring aggregate fraud levels much higher than the EEA average. For example, for 2022, some MS feature credit transfer fraud rates in value 10 times higher, or more, than the corresponding figures for the whole EEA. While there may be several underlying reasons for such differences across MS, including differences in the payment services offered by PSPs in the various markets, as well as the digital skills of citizens across MS, the EBA is of the view that this pattern might also be linked to the different implementation of the security requirements by PSPs and varying supervisory practices across MS.

23. As to the emerging fraud types, the EBA has observed that, unsurprisingly, fraudsters have started to adapt their techniques to the changed technological and regulatory context. As SCA has been successful in preventing fraud types based on the stealing of customers' credentials, new fraud types, of a more complex nature, emerged or became more widespread in recent years. These can be labelled under the following three categories:

    A. Manipulation of the payer. In this type of fraud, the customer is manipulated by a fraudster to make a payment to the fraudster through social engineering. These fraud techniques are arguably largely independent from technical security measures taken by the PSPs and usually leverage on information gathered on the customer e.g., via social networks, often making recourse to impersonation of a known and trusted party, like a relative, a friend, a business partner, tax authorities or the PSP itself. For the corporate segment, a typical example of such type of fraud is the so-called "CEO fraud", i.e. a fraud executed via phone or mail by a fraudster impersonating a high-level

business director or executive, manipulating an employee to initiate and authorise a payment, often for a large amount.

B. Mixed social engineering and technical scam. In this fraud type fraudsters combine phishing techniques (including vishing and smishing[8]), used to steal the customers' personal security credentials to gather account information and issue payment orders, with social engineering aimed at manipulating the PSUs to authorise the payment orders issued. Thus, while, impersonation of, say, a PSP's employee is often part of the fraud, as for the category above, it differs in that the fraudsters directly carry out some operations on the account of the victim. From fraud cases reported by NCAs and assessed by the EBA, it emerged that, when reporting this fraud type under the EBA GL on fraud reporting under PSD2, PSPs often categorize it as "manipulation of the payer", and consider the transaction as authorized, even if the payment order was issued by the fraudster.

C. Enrolment process compromise. This fraud type is a complex scam geared towards enrolling fraudster's devices as second factor of the SCA, to be used together with the customer's personal security credentials stolen by the fraudster via phishing/smishing/vishing techniques. In these scams, often leveraging on specific vulnerabilities of the enrolment procedures, the aim of the fraudster is taking over the payment account completely, thus enabling multiple fraudulent payments.

[8] While phishing refers to a scam perpetrated via email, in smishing fraudsters make recourse to SMS or instant messages and vishing takes place on a telephone call. Other techniques used by fraudsters include fake advertisements conveyed through common search engines, leading the victims to bogus websites mimicking the one of a trusted entity (e.g., a bank).

Specific proposals

24. The EBA welcomes the new security provisions included in the EU Commission's PSD3/PSR proposals and in the Instant Payments Regulation. In particular, the EBA welcomes the mandatory IBAN/Name check introduced by the Instant Payments Regulation, specifically as it applies also to cross-border transactions, as well as other additional fraud mitigation measures proposed by the EC in the PSR proposal - including enhanced transaction monitoring, supporting sharing of fraud-related information between PSPs and requiring PSPs to conduct educational initiatives to raise awareness of payment fraud among customers and staff. All of these can be useful, in particular, to mitigate manipulation of the payer fraud and other scams based on impersonation. Moreover, the EBA notes that additional provisions to mitigate fraud have been proposed in a report by the European Parliament's Economic and Monetary Affairs Committee (ECON) on the PSD3/PSR proposals and agreed by the European Parliament in a vote in April 2024 These aim, for example, at making electronic communications service providers outside the financial sector - e.g. telecommunications and internet providers, social media companies - also responsible for tackling payment fraud.

25. However, the EBA also notes that after 9 months from the entering into force of the Instant Payments Regulation, all PSPs in the Euro area will be required to accept instant payments, but only a part of them will support the IBAN/Name check. More generally, the phased application of the IBAN/Name check requirement to the EEA countries provided in the Instant Payments Regulation might lead, taking into account the aspects mentioned in paragraphs 17-18 above in relation to fraud for instant payments, to an increase of fraud levels during this intervening period, unless appropriate security safeguards are implemented.

26. Furthermore, considering the observed dynamic nature of fraud and the ability of fraudsters to adapt to new requirements aimed at combating fraud, the EBA is of the view that additional security measures – as articulated below - could be considered, with an aim at supporting a comprehensive, uniform and future-proof framework for the mitigation and control of payment fraud in the EU.

27. Based on the analysis summarized in the previous section and on an assessment of relevant measures to mitigate fraud reported by some NCAs as already in use in their jurisdictions, the EBA has identified the following additional measures for consideration by the EU co-legislators and the EU Commission in the negotiation of the PSD3/PSR proposals:

    1. Reinforced security requirements for PSPs, complementing the IBAN/name check and the fraud mitigation measures included in the PSD3/PSR proposals, aimed at further strengthening the procedure for the authentication of transactions, mitigating possible vulnerabilities exploited in other phases of the payment process, as well as supporting fraud detection and investigation;

    2. A fraud risk management framework to be put in place by PSPs, on top of the mandatory security requirements;

3. Amended liability rules, including a proper delineation between authorized and unauthorized transactions, as well as the clarification of the concept of "gross negligence";

4. A strengthened and harmonized supervision on fraud management, also leveraging on fraud data already collected under the PSD2;

5. Appropriate security requirements for a single EU-wide platform for information sharing to prevent and detect potentially fraudulent payment transactions.

28. The five suggested measures above are elaborated in more detail in the following subsections.

Reinforced security requirements for PSPs

29. The EBA arrived at the opinion that, taking into account the new and more complex fraud types emerging, a broader set of security requirements are needed for the provision of electronic payments. In this regard, the EBA suggests the following provisions for consideration by the EU co-legislators and the EU Commission in the discussion of the PSD3/ PSR proposals.

    a) With regards to the access to a payment account and the issuing of payment transactions/orders:

        i. Amending Art. 85(12) in the PSR proposal, to clarify that the two SCA factors should belong to at least two different categories, so as not to risk jeopardizing the positive effects SCA has had on fraud reduction;

        ii. A requirement for PSPs to offer the PSUs the possibility to set daily or per payment limits, below or above default values set by the PSP for each payment instrument, providing a proper delay for any resulting increase of spending limits to come into effect, but also respecting the spirit of recital 19 of the Instant Payment Regulation.

    b) With regards to the transaction monitoring (TM):

        i. A requirement that TM has to be performed before the execution of the transaction - i.e., for instant payments and other payments rapidly settled, in real time;

        ii. A clarification that TM should be applied to all electronic payment channels through which a given payment instrument is used by the PSU, inter alia though Automated Teller Machines (ATM) and at Points of Sale (PoS), thus making it possible to require the PSP to take an integrated view of the transactions processed for that payment instrument;

        iii. A requirement to complement the TM performed by the payer's PSP with the screening of received payment transactions by the payee's PSP, aimed at detecting suspicious fraud patterns based on, inter alia, the amount, origin, frequency of those transactions with respect to the profile of the account holder as well as possible deviation of the payee's name in transactions against the payee's name

held by the payee's PSP. Indeed, this measure is considered relevant to support the thorough monitoring by PSPs to fight fraud.

iv. A requirement for all PSPs to share fraud related information among themselves to enhance TM. In this regard, the provisions in Art. 83 of the PSR could be further strengthened by requiring all PSPs to share fraud related data, limited not only to unique identifiers/IBANs of the payee, but also including aspects such as other identification elements of persons suspected to be fraudsters (including names, IP addresses and phone numbers used) and information on the fraudsters' *modus operandi*;

v. A clarification that where, based on TM, a PSP determines an instant payment is high risk, it can refuse to execute the transaction with proper notification to the PSU, including the reason of the refusal, and the indication of the options available to re-issue the payment order. For other type of payments, whenever the TM indicates that the transaction is high risk, the PSP should carry out an investigation involving the counterpart PSP and may as a result of such investigation block the transaction. The details of this can be included in Level-2 legislation.

c) With regards to the procedure for the enrolment of a customer device as a second factor of the SCA:

i. To ensure an appropriate elapse of time from the PSU's request before the new customer device is effectively enrolled;

ii. In case of the enrollment of a further customer device, a requirement for PSPs to timely send an alert to the PSU's personal device already enrolled.

d) A requirement for PSPs to provide customer assistance with regards to any security aspects of the service and notification of anomalies and suspected fraud, including the possibility that the PSU promptly reaches out to trained staff and that the relevant case is timely followed up by the PSP, as needed. This service should cover at least the operating hours of the relevant payment service (i.e. the time span when the payment service is available to the PSU). This is without prejudice to PSPs' obligation under Art. 70(1)(c) of PSD2.

A fraud risk management framework to be put in place by PSPs

30. In addition to the above, the EBA advises the EU co-legislators and the Commission to set out requirements for a fraud risk management framework to be put in place by PSPs as part of the existing broader framework on risk management policies under PSD2 and Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA), in accordance with the principle of proportionality. Such framework could provide for periodical fraud risk assessment, based, inter alia, on the fraud data collected under the PSR and include:

a) A fraud risk statement by PSPs, setting out the objectives of containment of fraud, to be regularly revised;

b) a regular monitoring by PSPs of own fraud levels, both on the payer's PSPs side and the payee's PSP side.

c) the regular update of the security measures implemented to mitigate the risk of fraud, based on the fraud rate detected and the assessment of the relevant risk faced.

Amended liability rules

31. The EBA advises the EU co-legislators and the EU Commission to clarify the liability rules in the PSR proposal, and in particular:

a) To clarify the delineation between authorized and unauthorized transactions in case of disputes about a suspected fraud between the PSU and the PSP. In particular, the following measures could be considered:

i. to specify in the PSR that, where a payer denies having authorized a transaction, the use of SCA should not in itself be sufficient to prove either that the payment transaction was authorized by the payer or that the payer acted fraudulently;

ii. to specify that, in case of payer-initiated transactions (e.g., credit transfers), a transaction denied by the payer cannot be considered as authorized where the payment order was initiated by a fraudster, even if it was subsequently authenticated by the PSU;

iii. to clarify that, without prejudice to Art. 5(c)(8) of the Instant Payments Regulation, a transaction denied by the payer cannot be considered as authorized where the payer was not made aware of a mismatch between the IBAN and the name of the beneficiary, including, e.g., because the fraudster has intercepted the notification from the payer's PSP referred to in Art. 5(c)(1) of that Regulation.

b) To clarify the concept of gross negligence. In this regard, the following measures could be considered:

i. to clarify in the recitals to the PSR that, where a PSU falls victim of social engineering fraud, in order to assess whether the PSU has acted with gross negligence, account should be taken of all relevant factors, including but not limited to the complexity of the fraud, the personal circumstances of the PSU, whether the latter had reasonable grounds for believing that the PSU was making a payment to a legitimate payee, and whether the PSP could have taken additional steps to help prevent the fraud taking place.

ii. to include in the recitals of the PSR a non-exhaustive list of circumstances that could be taken into account when assessing gross-negligence, such as:

- the PSU has made a payment to a fraudster without having any reasonable grounds for believing that the payee to whom the payment was intended is legitimate;

- the PSU has made their personal security credentials, including where applicable the devices or elements used for the second factor of authentication, openly and easily available to the fraudsters;
- the PSU has already been a victim of the same manipulation of the payer or social engineering fraud type and *modus operandi* before;
- the PSU has disregarded warnings regarding the specific fraud type experienced, recently addressed to the PSU following the outcome of TM and/or related investigations by the PSP;
- the PSU has not timely notified the fraud to the PSP upon becoming aware of it.

c) To specify that PSPs are liable for fraud, inter alia, when:

i. they failed to fulfil their obligations to provide the PSU with customer assistance with regards to security, as articulated in paragraph 29(d) above, in relation to the fraud experienced;

ii. the fraudster has accessed the PSU's personal or account information following a data breach at that PSP, including of the kind set out in Art 9(3)(c) DORA, prior to the fraud.

32. In the EBA's view, the changes proposed above would help to ensure more effective consumer protection, while reinforcing the responsibility of PSPs for the security of the payment services offered. These changes would also reduce the relevant costs of disputes management, for PSPs and customers alike.

Strengthen and harmonize the supervision of fraud management

33. The EBA advises to strengthen and harmonize the supervision of fraud management, leveraging on supervisory best practices used in some MS, as well as the fraud data collected under the reporting framework already implemented under the PSD2. To achieve this, further requirements in the PSR could be considered, such as requiring NCAs to:

a) regularly monitor fraud data collected from the relevant PSPs at national level - on the side both of the payer's PSP and the payee's PSP, verifying that the overall fraud rates for all the main payment instruments are kept well below appropriate maximum tolerable levels set at EU level, taking into account statistical fraud data available under the EBA GL on fraud reporting under PSD2;

b) based on the outcome of the abovementioned monitoring, follow up possible outliers, i.e. PSPs featuring fraud level over or close to the mentioned maximum tolerable levels, and take possible supervisory actions, as appropriate.

c) regularly monitor the correct recourse to MITs and MOTOs by PSPs, as well as the compliance of the application of SCA and SCA exemptions by PSPs.

Security requirements for a single EU-wide platform for information sharing

34. In addition to the suggestions outlined in paragraph 29(b) above as regards fraud transaction monitoring and the fraud data sharing amongst PSPs envisaged in Art. 83 of the PSR proposal, the EBA advises the EU co-legislators and the EU Commission to consider further strengthening Art. 83 of the PSR proposal with a requirement to have a single EU-wide platform, to be maintained and run by PSPs, for the sharing of fraud data amongst PSPs, in order to fully capture the benefits of the measure.

35. Moreover, consideration could be given to specifying appropriate security standards for the treatment of unique identifiers of payees and other fraud related data to be exchanged by PSPs under Art. 83 PSR, taking into account personal data protection requirements. In particular, consideration could be given to specifying that suspicious unique identifiers (e.g., IBANs) or other personal data that should not be shared among PSPs, but notified by the latter and stored in the platform as cryptographic hashes. The verification of the match of an incoming personal identifier of the beneficiary of a given transaction, could be done automatically in the platform by confronting it with the list of hashes already stored, without any exchange of personal information among PSPs and without any treatment of customer personal or sensitive information in clear in the platform itself.

36. Furthermore, to support collaboration among PSPs in the follow-up and investigation of fraud, the data to be exchanged by PSPs via the above-mentioned platform could include, in addition to the aspects mentioned in paragraph 29(b) above, a list of contact points of all PSPs.