SMART2

SCT Inst Migration Action Round Table

Best practices to support PSPs in detecting/combatting fraud and scam

SMART2 recommendations – version 1.0 of 18/06/19

Introduction

The SCT Inst Migration Action Round Table (SMART2) has put together the present note to help improve measures at PSP level geared at detecting and combatting fraud and scam. The objective is to support the development and use of uniform practices at a pan-European level, both at inter- and intra-PSP level. The underlying aim is to assist account-holding payment service providers (AS-PSPs) and, where applicable, third-party providers[1] in ensuring a smooth, uniform and – above all – safe customer experience.

It should be stressed that while many of the below-mentioned best practice recommendations would benefit from being applied to other payment instruments and some could even be considered for roll-out at a global level, they are particularly relevant for instant payments in an integrated payments landscape, such as the SCT Inst Scheme in the Single Euro Payments Area, due to the increased speed these transactions have brought to the payment execution and related cash-out processes.

Furthermore, it is worth mentioning that putting into practice these recommendations would also help to reinforce anti-money laundering and counter-terrorist financing activities in the payment environment.

Approach and definitions

The present note distinguishes between

- practices to be implemented at AS-PSP-internal level,
- practices that would require collective action at inter-PSP level and/or at infrastructure level for a positive impact,
- measures that would require actions at public authority or law enforcement level.

Where relevant, the note further distinguishes between “fraud” (where a third person fraudster initiates an unauthorised transaction) and “scam” (where the payer is manipulated into taking an action). In detail, this distinction is based on the following two definitions established by Guideline 1.1 of the European Banking Authority’s Guidelines on reporting requirements for fraud data under Article 96(6) PSD2:

- Fraud would be defined as “unauthorised payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer (‘unauthorised payment transactions’)”

[1] It should be noted that not all recommendations in this note are applicable to third-party providers (TPPs) that may be involved in the initiation of a payment transaction.

- Scam would be defined as “payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee (‘manipulation of the payer’).”

While the distinction at PSP level between fraud and scam is vital in a number of circumstances because the two approaches require different detection and follow-up measures, it is important to note that in the remainder of the note, “fraud” is used as a general, overarching expression encompassing both scam and actual fraud.

Practices at PSP level

- Ensure state-of-the-art processes for customer onboarding and the related know-your-customer checks
- Enhance customer behaviour profiling, conducting:
  - (technical) frontend profiling of customer usage patterns for mobile devices, browsers etc., covering a large number and wide range of technical attributes
  - (business) backend profiling of customer transactions
  - additional third-party provider (TPP) profiling:
    - TPP profiling at customer/account level
    - TPP profiling across different banking group entities
- Centralise fraud alert handling and customer interaction in a dedicated 24/7 specialised team focusing both on payment and credit/debit card fraud. This centralisation effort should ideally also involve the set-up of one central risk engine for profiling and scoring transactions across services. This should make fraud profiling and scoring more effective and help avoid the proliferation across multiple channels of fraud cases related to the same customer.
- Develop the necessary abilities to detect and distinguish scam and fraud (see definitions provided above)
- Implement automated, real-time (especially for instant payments – ideally prior to strong customer authentication) and differentiated customer interaction
  - for scam: automated information/challenging via the same channel with a dedicated set of scam-specific questions
  - for fraud: automated information/challenging via a separate channel and (different) dedicated set of fraud-specific questions
- Enhance monitoring of both incoming and outgoing payment flows on customers’ payment accounts
- Introduce SCA solutions that are both risk-based (establishing fraud risk based on technical attributes) and dynamic (e.g. not always requiring the same sequence of SCA steps)
- Ensure that customers are kept aware of and educated about fraud-related risks and prevention measures

Practices at inter-PSP and/or infrastructure level

- Put in place an ideally pan-European fraud scoring solution at PSP level that allows the payer's PSP to provide a fraud score for outgoing payments, preferably in the payment message itself, to support the payee's PSP in its inbound fraud detection activities, without entailing any liability shift. Such solutions are currently being piloted or pioneered at national level in different communities[2]. For optimal results and potential alignment, any work on defining a pan-European fraud scoring approach should take into consideration these solutions and related first usage experiences. A potential next step on this topic could be the submission of a change request for a pan-European fraud scoring approach to the European Payments Council by 31 December 2019 in view of the SEPA Scheme Rulebook updates for 2021.
- Define a "request for blocking of beneficiary account" message and fraud investigation/information messages in ISO 20022 format, which could serve as a more effective alternative to an emergency contact list in case of scam/fraud-related issues causing the cancellation.
- Define a standard set of data elements and a related ISO 20022-based transmission format for the exchange of contextual information (e.g. the information that this is the first time this payer sends a payment to this payee account) between payer's PSP and payee's PSP to facilitate fraud detection activities at beneficiary PSP level.
- Define and implement supportive fraud detection measures at central infrastructure level, to identify for instance fraud-related funds transfers across financial institutions, e.g. cash-outs based on consecutive sending of SCT Inst transactions from one account to the next.
- Establish a forum at a pan-European level enabling the exchange and discussion of recent and relevant fraud case experiences and the communication of any related conclusions or guidance to relevant stakeholders.

Measures at public authority or law enforcement level to support fraud detection and combat

- Provide AS-PSPs with the possibility to run specific checks against public authority databases in order to minimise identity risk during the customer onboarding process and thus ensure better KYC efficiency. Such limited checks are already supported in a number of European countries today.
- Provide AS-PSPs with the possibility to run checks against a national or, ideally, pan-European database or information service regarding stolen/defrauded identity documents (e.g. passports, national ID cards, drivers' licenses), which could be done as part of the payment initiation/execution process.
- Put in place (or support the creation of) a pan-European database of IBANs and related account holder names against which PSPs could run checks as part of the payment initiation process to validate that there is an IBAN/account holder name match. Such solutions already exist or are in the process of being delivered at national level in some European countries.[3] Whether any existing or emerging solution(s) could be evolved or combined into a pan-European approach remains to be investigated. Alternatively, to avoid

[2] For a non-exhaustive overview list of national fraud scoring solutions and references to more information, please consult Annex 1 of this document.

[3] For a non-exhaustive overview list of national solutions enabling an IBAN/account holder name check and references to more information, please consult Annex 2 of this document.

the build-up of a central database, this check could be performed based on a validation request sent by the payer's PSP to the payee's PSP.

- Create (or support the creation of) a pan-European fraud-related register or information service to share fraudulent/suspicious IBANs or run checks against[4], as part of the payment initiation/execution process.[5]

Conclusion and way forward

As the present note reflects, detecting and combatting fraud (and scam) activities in payments requires the deployment and combination of a wide range of measures at different levels. To successfully implement many of the proposed best-practice measures listed above, PSPs need to start by adapting and investing in their internal processes.

At the same time, the note also makes it clear that the effectiveness of such measures highly depends on the quality of the co-operation of and interaction between the different market players involved in a payment transaction. It begins at the interaction with the payment service user (which is not part of the main scope of this note) and extends to the interaction between PSPs as well as between PSPs and the infrastructure solutions they rely on. As the proposed measures in that section show, this inter-PSP interaction can be enhanced significantly from a fraud detection perspective through the joint definition and implementation of measures fostering information exchange on fraud-related topics. This point is widely recognised and at the basis of collective industry initiatives such as the European Payments Council's Payment Security Support Group.

However, it cannot be stressed enough that successful fraud combatting and detection also heavily depend on the creation and nurturing of a supportive ecosystem. Many information elements that would enable effective fraud detection by PSPs are today either held by public authorities or cannot be easily exchanged between PSPs, especially at a pan-European level, due to the lack of a sound and uniform legal framework that could be the basis for this exchange. One of the purposes of this note is to encourage the parties concerned to engage in a dialogue aimed at exploring possibilities to foster the development of fully automated and efficient pan-European solutions in this area, as well as of the necessary legal basis for these solutions.

In closing, it is important to emphasise that the strengthening of fraud prevention and detection activities at the level of individual institutions and through industry-wide efforts should not only help to make existing and new payment products safer – the recommended measures should, above all, contribute to making their usage as easy and convenient for end-customer as possible.

***

[4] For a non-exhaustive overview list of fraud-related registers and references to more information, please consult Annex 3 of this document.

[5] Regarding the set-up of the databases/registers mentioned under this and the previous bullet point, due consideration would need to be given to the requirements of the General Data Protection Regulation. Considerations may involve the question whether the inclusion of IBAN/account holder name in the database could rely on legitimate interest as legal basis (in accordance with GDPR Recital 47: "The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned."), provided that the relevant legitimate interest assessment leads to such conclusion, or whether a different legal basis from those foreseen in the GDPR, in particular the legal obligation to prevent fraud which the controller is subject to, would rather apply.

List of endorsing AS-PSPs

This note has been created by participants in the SCT Inst Migration Action Round Table (SMART2), an infrastructure-agnostic forum aimed at dealing with issues of an operational nature impacting a smooth end-to-end execution of instant payments in SEPA that might benefit from joint analysis and exchange.

For more information about SMART2, please consult:

https://www.abe-eba.eu/market-practices-regulatory-guidance/sct-inst-migration-round-table-smart2/

The note has been endorsed by experts of different divisions, including payments, compliance and fraud detection departments, of the following account-servicing payment service providers (AS-PSPs) operating in Europe:

ABN AMRO

Bank of Ireland

BBVA

BCEE

BIL

CaixaBank

Deutsche Bank

DNB Bank

Erste Group Bank

Handelsbanken

Helaba – Landesbank Hessen-Thüringen

Nordea

Raiffeisen banka a.d. Belgrade

RBI

Standard Chartered Bank

Contact details

For any comments or questions concerning the above note, please contact the Secretariat of the SCT Inst Migration Action Round Table at association@abe-eba.eu.

Annex 1: non-exhaustive overview list of national fraud scoring solutions and references to additional information

- The Netherlands:
  For more information regarding the Dutch Fraud Indication Marker solution for SCT Inst (providing a fraud score for outgoing payments in the payment message itself without entailing any liability shift), please contact Betaalvereniging Nederland (Dutch Payments Association) at: naso@betaalvereniging.nl

Annex 2: non-exhaustive overview list of national solutions enabling an IBAN/account holder name check and references to additional information

- Netherlands:
  SurePay solutions “IBAN-Naam Check” (https://www.surepay.nl/en/services/account-check/) and “API for organizations” (https://www.surepay.nl/en/services/batch-check/)
- United Kingdom:
  SurePay solution “Confirmation of Payee”
  (https://www.surepay.nl/en/services/confirmation-of-payee/)

Annex 3: non-exhaustive overview list of fraud-related registers and references to additional information

- Nordics:
  Nordic Financial Cert (NFC, https://www.nfcert.org/). The aim of the online portal is to share relevant data to combat cybercrime; no personal data is shared except for account numbers; Banks can only report account numbers or IP addresses if a fraud case involving this data has been confirmed; no other personal data is shared.

- Netherlands:
  If a bank detects a potential fraud case, the supposedly fraudulent IBAN will be put onto a dedicated server the other Dutch banks interface with, in order to pull in this information; each piece of information is only made available for 14 days. The way forward of this solution is currently under review.