Market Practices & Regulatory Guidance

GIFT CARDS: A GIFT FOR FRAUDSTERS?

A SMART2 paper on the abuse potential of closed-loop cards

SMART2

SCT Inst Migration Action Round Table

Market Practices & Regulatory Guidance

GIFT CARDS: A GIFT FOR FRAUDSTERS?

A SMART2 paper on the abuse potential of closed-loop cards

SMART2

SCT Inst **M**igration **A**ction **R**ound **T**able

Content

INTRODUCTION

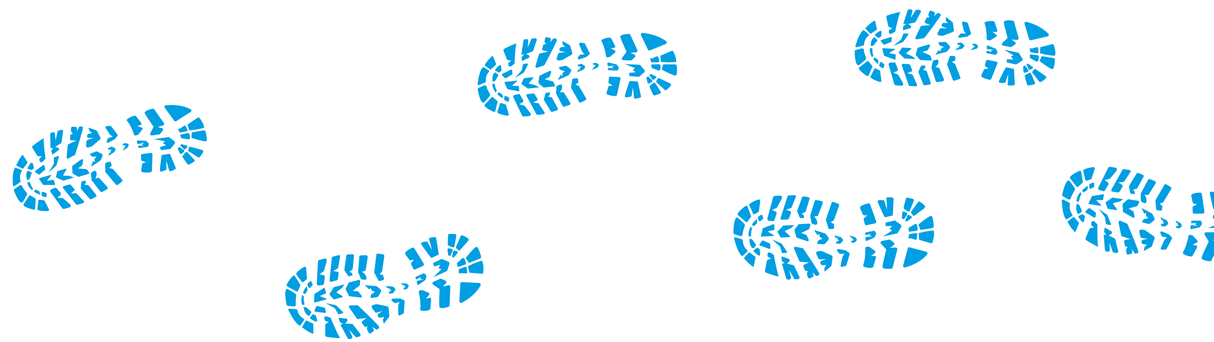
Anonymous prepaid cards have attracted increasing regulatory attention over the past few years in Europe and beyond. Most recently, the AML5 Directive has further shut the gates on the fraudulent use of such cards by tightening the rules around their use. It has, for instance, further reduced the maximum amount that can be charged on such a card.

However, the restrictions set by the AML5 Directive or the E-Money Directive only apply to so-called general-purpose or open-loop cards. Closed-loop gift cards and other limited-purpose tokens, the use of which is restricted to a specific environment, are not subject to the same requirements.

Gift cards are very attractive both for merchants and their customers as testified by the growing revenues they generate: the global gift cards market size was valued at $ 619.25 billion in 2019 and is projected to reach $1,922.87 billion by 2027, growing at a compound annual growth rate of 15.4% from 2020 to 2027[1]. But gift cards have not only been among the most popular items on consumers' year-end holiday wish lists for the past decade[2] – the closed-loop type, in particular, is also tremendously popular among fraudsters.

Because of their characteristics, closed-loop cards are an ideal instrument for criminals to cover up their tracks when laundering money or defrauding victims of their funds. As such gift card purchases frequently involve the use or abuse of a payment instrument or account, the fraud victims holding these accounts or instruments usually turn to their payment service providers (PSPs) for help. Unfortunately, the conversion of funds into gift cards generally makes it impossible for these institutions to follow and claim back the money for their customers.

The present paper explains why closed-loop cards still hold a huge potential for fraudsters. It also highlights key scenarios, as identified by banks and their customers, where these cards are used for fraudulent purposes today. The paper has been prepared by fraud experts from banks across Europe contributing to the SCT Inst Migration Action Round Table (SMART2) hosted by the Euro Banking Association. The aim of the paper is to raise additional awareness around this abuse and to help further curb it going forward.



1 https://www.alliedmarketresearch.com/gift-cards-market

2 https://nrf.com/media-center/press-releases/holiday-shoppers-plan-spend-4-percent-more-year

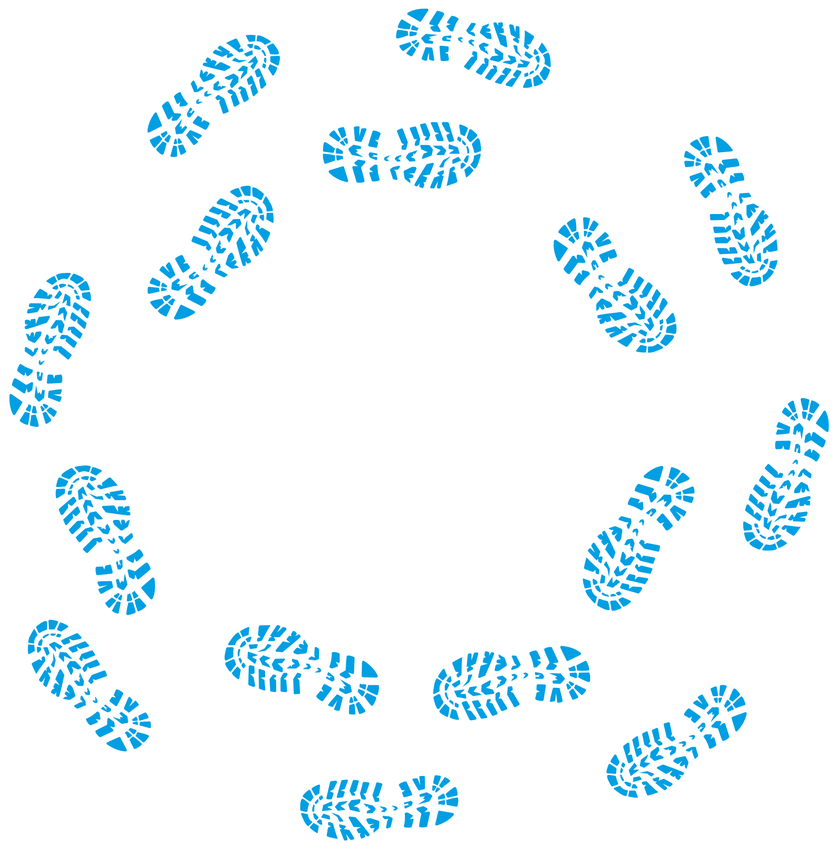
CLOSED-LOOP CARDS: WHAT ARE THEY AND HOW THEY ARE USED?

Closed-loop or limited-purpose cards [3], such as gift cards, store cards, petrol cards or casino cards, are payment instruments that in essence can be used "to acquire goods or services only in the premises used by the issuer" or "within a limited network of service providers" or "for a very limited range of goods or services".[4]

The amount charged on a closed-loop card is paid upfront by the customer before the card is activated. The card issuer becomes immediately the owner of the amount loaded to the card, which in turn allows the customer to spend the amount among a closed group of merchants or stores. A closed-loop card does not provide access to an automated teller machine (ATM) network, which means there is no direct channel for cashing out any funds stored on these cards.

Closed-loop cards can easily be purchased in physical stores, on many merchant websites or in online casinos. Since closed-loop cards do not carry the name of the customer using the card, but only the brand of the merchant or chain of stores where the card can be used, closed-loop cards are an anonymous payment method. The person who purchases such a card online usually only needs to register an email address or link to his or her social media profile.

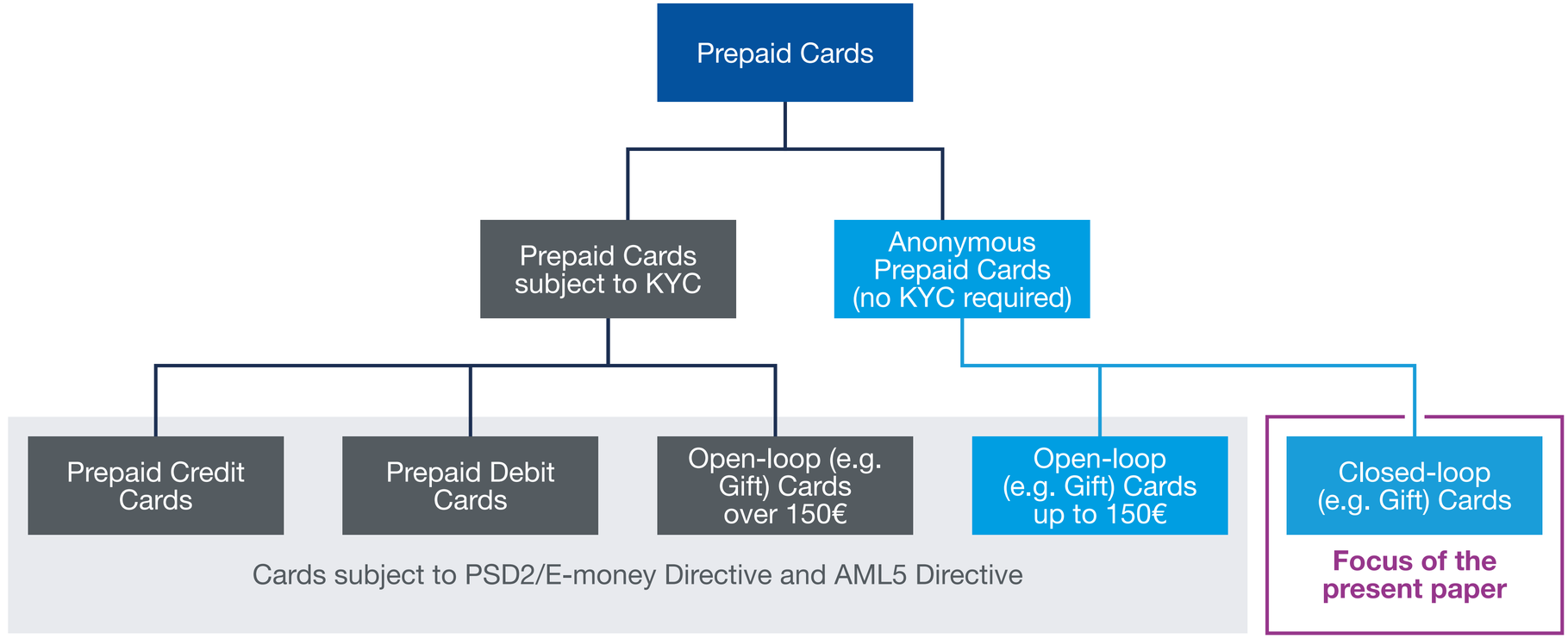
After having registered, the person simply makes a payment to charge the card. This payment can be initiated through credit or debit cards, online e-money services or through a money transfer from an internet banking account. Depending on the underlying terms and conditions, some of these closed-loop cards, such as gaming or casino cards, can be topped up.



3 While cards are the most commonly used limited-purpose token, the term "card" as used in this paper should also be seen as a stand-in for other tokens that work in a similar way, e.g. online casino tokens.

4 Directive (EU) 2015/2366 on payment services in the internal market (PSD2), amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, Art. 3(k)(i)(ii)(iii), Recital (13).

OVERVIEW OF DIFFERENT PREPAID CARD TYPES AND RELATED REQUIREMENTS



HOW ARE CLOSED-LOOP CARDS REGULATED IN EUROPE?

Since they are issued in a strictly closed-loop environment, these cards do not require compliance with the PSD2 or the E-money Directive[5] in relation to prepaid cards. Since they are no e-money product, they would not attract the application of the requirements and limits defined by the AML5 Directive with respect to electronic money.[6] From this, it can be deferred that the maximum limit of EUR 150 defined by the AML5 Directive does not apply to closed-loop cards that meet the conditions of Article 3(k) PSD2.[7] However, some aspects of these cards and/or the related commercial agreement with the issuer may be subject to specific other requirements which do not stem directly from the AML5 Directive.

The maximum limit of a closed-loop card is set by the entity issuing the card. Depending on the merchant, it generally varies from EUR 50 to EUR 1,000 per card. That means that comparatively high amounts of money can be stored on this type of cards. An obligation for the card-issuing entity to apply customer due diligence measures, such as validating and/or registering the identity of the customer, only kicks in if a customer buys gift vouchers for more than EUR 10,000 in cash.[8]

5 E-money Directive (Directive 2009/110/EC), Art.1(4) referring still to Art. 3 (k) PSD1 (Directive 2007/64/EC) which is to be read (in accordance with Art. 114 PSD2) as a reference to Art. 3(k) PSD2 (Directive 2015/2366/EU) which entered into force on 12 January 2016 and replaced PSD1 on 13 January 2018.

6 AML4 Directive (Directive 2015/849/EU as amended), Art. 3 (16) excluding from the scope of electronic money considered by the directive, “monetary value as referred in Art. 1(4) [of the E-Money Directive]”.

7 Directive (EU) 2018/843 of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU (“AML5 Directive”), Art. 1, para 7, point (a).

8 Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012, repealing Directive 2005/60/EC and Directive 2006/70/EC (“AML4 Directive”), Art. 2, para 1 (e).

COMPARISON OF OPEN-LOOP VS. CLOSED-LOOP CARDS

	Open-loop cards	Closed-loop cards
EXAMPLES	Prepaid credit and debit cards, open loop gift cards	Gift cards, store cards, petrol cards, casino cards
ACCEPTANCE	Open-loop gift cards: Large number of different merchants or acceptance points Anonymous prepaid credit or debit cards: acceptance identical to regular credit and debit cards	Used to acquire goods or services within a limited network of service providers / closed group of merchants or stores
USAGE	Can be used for payments both online and in-stores Amount charged on card paid upfront by customer	Can be used for payments in-stores and/or online Amount charged on card paid upfront by customer
ACCESS TO ATM?	Prepaid credit or debit cards provide access to an ATM (you can withdraw money with the card)	Does not provide access to an ATM
DUE DILIGENCE MEASURES REQUIRED?	Subject to customer due diligence (CDD) measures or partial CDD exemption (see "Anonymity"). Ongoing monitoring and reporting of suspicious transactions are mandatory for all of these cards.	Due diligence measures only necessary if customer buys cards for more than EUR 10,000 in cash
CAN CARDS BE RELOADED?	Prepaid credit and debit cards can be topped up	Usually for a one-time use, but some cards such as gaming or casino cards can be reloaded
REGULATED?	Open-loop cards are defined as e-money* and are therefore regulated by the E-money and AML5 Directives	PSD2 and E-money Directive as well as e-money requirements of AMLD5 not applicable
MAXIMUM LIMIT THAT CAN BE STORED	No maximum limit defined by regulation if customer due diligence measures were undertaken; for anonymous open loop prepaid cards, the maximum amount is EUR 150 (see "Anonymity")	No maximum limit set by regulation but by entity issuing the card (generally varies from 50 to 1000 EUR)
ANONYMITY	According to the AML5 Directive, the anonymous use of prepaid cards is only permitted if the following circumstances are met**: ⊕ the maximum amount stored on the card does not exceed EUR 150 ⊕ the card is not reloadable or has a monthly spending limit of EUR 150 which can only be used in the EU member state where the card is issued ⊕ the payment instrument is used exclusively to purchase goods and services ⊕ anonymous e-money is not used to fund the card ⊕ any redemption in cash or online transactions does not exceed EUR 50 per transaction EU member states are also required to ensure that anonymous prepaid cards issued outside the European Union are not used on European territory unless they meet requirements equivalent to those mentioned above.	Anonymous means of payment
PROTECTION AGAINST LOSS OR THEFT	Open-loop cards: normally no protection Prepaid credit and debit cards: similar to regular credit or debit cards, i.e. blocking of card possible	Normally no protection

* Art. 2(2) of E-Money Directive ** Art. 1(7) of AML5 / Art. 12(1) of AML4

WHICH CHARACTERISTICS MAKE CLOSED-LOOP CARDS ATTRACTIVE FOR FRAUDSTERS?

a. Little to no customer due diligence process

A consumer purchasing a closed-loop prepaid card usually does not have to undergo a customer due diligence process (also known as know-your-customer or KYC process).

b. Anonymous means of payment

Since a closed-loop card does not bear the name of the customer using the card, but only the brand of the merchant or chain of stores where the card can be used, customers can pay with this type of cards in an anonymous way.

c. Possibility to store relatively high amounts of money

The maximum amount of money that can be loaded and stored on a closed-loop card is set by the entity issuing the card, i.e. there is no maximum limit stipulated by European law. Depending on the merchant, the limit generally varies from EUR 50 to EUR 1,000 per card. Some cards are sold with a pre-defined amount while others allow the customer to flexibly determine the amount (up to the maximum limit) when purchasing the card.

d. Dematerialisation possible (using string of characters rather than physical card)

Closed-loop cards can exist in a dematerialised way, which means that the customer does not necessarily have to be in possession of the physical card to initiate an online transaction but just uses a string of characters linked to the card.

e. Portability

Closed-loop cards can be used very much like cash, since they are not registered to a person and can easily be passed on to someone else. Anyone in possession of the card (or the related string of characters) is able to directly use it as a payment means within the closed environment where the card is valid.

f. Refund of the money possible in certain cases

Some issuing parties (e.g. online casinos) offer the possibility to refund closed-loop cards, i.e. exchange the card for money if the underlying terms and conditions of the card as defined by the issuers allow it.

g. Acceptance of closed-loop cards as cash equivalent outside closed environment

Due to the anonymous character, the portability and the limited cancellation risk of the card, closed-loop cards of widely-known and well-trusted merchants are accepted as cash equivalents in a lot of contexts, i.e. they can be traded in for other cards, vouchers or goods outside the environment for which they were issued. They can also be easily turned into cash if sold over an online gift card resale site at a small loss.

h. Limited/no cancellation risk

Most issuers do not offer a process that would allow third parties to notify the issuer about any abuse of the card. Furthermore, the purpose of a 'gift card' is giving it to someone else which is why such cards are generally not tied to the identity of a specific customer. As a result, there is usually no way of verifying whether a card has been passed on to a different user. Given these limitations, it is not surprising that most issuers have no cancellation or blocking process in place for the cards they issue, which could be applied in case the card has been lost or abused.

WHAT ARE THE MOST COMMON FRAUD CASE SCENARIOS INVOLVING CLOSED-LOOP CARDS?

In the payment fraud space, closed-loop cards are most frequently used in the following common fraud scenarios:

- as a means of obtaining money from a victim through so-called gift card scams
- as a 'cash-out' transaction following fraudulent access to a victim's funds or payment means

How does the gift card scam scenario work?

In a gift card scam, fraudsters try to get gift cards instead of any other form of payment or benefit they would usually try to receive from the victim. The scam generally works like this:

- The fraudsters approach their targets impersonating an authority requesting immediate payment of a due amount (e.g. taxes or fines) or a person or institution requiring urgent financial support.
- The fraudsters pressure or manipulate their targets into buying gift cards or other closed-loop cards and providing the gift card codes or numbers to the fraudsters.
- Once the fraudsters have obtained the code or gift card numbers from their victims, they liquidate the funds by buying goods that can be remonetised on the black market or through small back alley stores all over Europe. These goods follow basically the same circuits as stolen goods. In some cases, the fraudsters sell the gift card numbers they have obtained on gift card resale sites instead of buying goods that can easily be resold.

How does the cash-out scenario work?

In the cash-out scenario, the fraudsters use a fraudulently obtained access to funds for the purchase of gift cards, so that their transactions cannot be traced. Possible fraudulent actions that precede the purchase of closed-loop cards may involve the following:

- a phishing attack leading to the takeover of a payment account or online shopping account
- the use of a stolen debit or credit card or of stolen card details

The fraudsters use the card (details) or the taken-over account to purchase closed-loop cards, which are then turned into cash in the same way as described earlier.

WHAT ARE THE KEY ADVANTAGES OF CLOSED-LOOP CARDS FOR FRAUDSTERS?

Closed-loop cards are actively used by fraudsters because they combine major advantages of cash (portability and inherent anonymity) with the key benefit of virtualisation (tokenisation). What makes these cards even more attractive for fraudsters is that they can carry relatively high maximum amounts of money. Furthermore, closed-loop cards hold the following benefits for fraudsters:

- Fewer money mules are needed: any number of cards can be directly purchased from different providers worldwide through payments from a taken-over account or with stolen card data. Fraudsters are not required to start campaigns in order to look for money mules, and the money mules do not get burnt in the cash-out process.[9]
- The anonymity and portability of the cards offer fraudsters the possibility to disperse the cards all over their network or, when larger sums are required, to bring all cards together in the hands of one single player, while the usage of the card cannot be traced to this single player.
- As soon as the funds are loaded upon such cards, the money effectively leaves the traceable circuit and its behaviour becomes comparable to cheques or cash, i.e. untraceable.
- Tokenisation of these cards: a lot of these cards do not need to be physically present in order for a person to pay with them and they can be used as long as the expiry dates of the cards have not passed.[10] As a result, a single data file as such can contain many thousands of numbers for closed-loop cards (with related expiry dates), which can easily be used all over the globe.

9 While anonymous closed-loop prepaid cards can be used to **replace** money mules in the cash-out process, anonymous **open**-loop prepaid cards are often used in the same context because they **hide** that the transfer goes to a money mule: these debit/credit cards are topped up via transfers to a money bin held by the card issuer, which means that the beneficiary IBAN is the IBAN of the money bin and the beneficiary name is the name of the card issuer. The number of the card that is being topped up only shows up in the remittance data field, which makes it impossible for the originator bank to identify the beneficiary or classify the beneficiary IBAN as belonging to a mule account.

10 Most jurisdictions require that gift cards are sold with a mandatory minimum expiry period of three years.

WHAT COULD BE DONE TO CURB THE ABUSE OF CLOSED-LOOP CARDS?

As detailed above, closed-loop cards have a number of characteristics that make them highly attractive for fraudsters. These features allow criminals to swiftly cover up their tracks when laundering money or defrauding victims of their funds, and to easily convert these funds into assets that can be managed very simply and conveniently.

When financial institutions detect (or are informed by their customers about) the underlying fraudulent action or the related scam, they are usually unable to follow and claim back the money for their customers because of its conversion into gift cards. In most cases, it is impossible for payment service providers (PSPs) to infallibly identify that a fraudulent card transaction or a payment transaction following an account takeover has resulted in the purchase of closed-loop cards or tokens. But even if that link has been clearly established, there is often not much a PSP or its customer can do: for the vast majority of closed-loop cards, an effective follow-up on such abuse cases is prevented by the lack of reimbursement and cancellation policies applicable to these cards.

In contrast to cases within the payments ecosystem, i.e. where the account takeover results in a credit transfer to another payment account (usually held by a money mule), there is also no established investigation and co-operation approach in place for impacted parties, neither for compensation nor for fraud fighting purposes. There may be occasional co-operation initiatives set up by individual payment service providers and local merchants, but these only address a tiny fraction of the actual abuse cases.

In closing, it is important to stress that closed-loop cards currently represent a challenge that fraud fighters find difficult to tackle. What has turned these gift cards and tokens into a ‘gift’ for fraudsters is that they feature all the benefits of ‘cashless cash’ without facing the low maximum amount limit and further regulatory restrictions that other anonymous prepaid cards are subject to. While their lack of traceability makes it very difficult to quantify the extent of the issue and of the damage caused by the abuse of these cards, fraud experts from financial institutions across Europe agree that this would be a security loophole worth closing – for the benefit of their impacted customers as well as anti-fraud and anti-money laundering efforts across and beyond the payments ecosystem.

"a challenge that fraud fighters find difficult to tackle"

IMPRINT

Euro Banking Association
40 rue de Courcelles
F-75008 Paris

CONTACT

association@abe-eba.eu

GRAPHIC DESIGN

Bosse und Meinhard, Bonn

IMAGES/ILLUSTRATIONS

istock/DEVASHISH_RAWAT; istock/NiseriN; istock/olegback; Noun Project; composing: Bosse und Meinhard

About the SCT Inst Migration Action Round Table (SMART2)

The SCT Inst Migration Action Round Table (SMART2) is an infrastructure-agnostic forum for account-servicing PSPs geared at bringing clarification to instant payment migration-related issues and to work towards defining industry best practices and publishing common positions based on a consensus among the participants, where needed.

The forum is logistically supported by the Euro Banking Association and provides a facility for consultations on 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.

The present paper is based on input provided by the participants of the SMART2 sub-group on instant payment transaction screening and fraud detection practices. Editorial and administrative support has been provided by Annick Moes and Andreas Kirchmann from the Euro Banking Association.

More information about SMART2 can be found at

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