A pan-European fraud taxonomy: Do you speak fraud?

Received (in revised form): 22nd January, 2024

Annick Moes*
Head of Industry Issues, Cooperation Initiatives and Communications, Euro Banking Association, France

Meral Ruesing**
Communications Expert, Euro Banking Association, France

Annick Moes *is Head of Industry Issues, Cooperation Initiatives and Communications at the Euro Banking Association (EBA), the largest cross-sectoral network of payment practitioners pursuing a pan-European vision. Annick is responsible for the EBA's market practices and regulatory guidance stream, which provides the European payments ecosystem with a pan-European perspective and practical support. Prior to joining the EBA Group in 2003, Annick worked in journalism and market research in the EU and the USA.*

Meral Ruesing *serves as Communications Expert at the Euro Banking Association (EBA). Meral is the Rapporteur of the EBA Expert Group on Payment Fraud-related Topics, which developed the EBA Fraud Taxonomy. Prior to joining the EBA, Meral held positions with the Global Legal Entity Identifier Foundation, the European Payments Council and the Association of German Banks.*

ABSTRACT

Understanding the myriad activities of fraudsters, and finding effective measures to rapidly counteract them, continues to be a vexing problem for payment service providers (PSPs) — a challenge that is being intensified by the move to a 24/7/365 and real-time payments environment. To strengthen the fraud detection and prevention tools available to PSPs, there are growing efforts within the industry to create a pan-European ecosystem for sharing fraud data and intelligence, facilitated by regulatory and legislative developments. To ensure that the benefits of these new tools can be fully reaped, this paper argues that there is a need for PSPs to get their own houses in order by harmonising the fragmented fraud terminologies and internal reporting requirements in practice today. By leveraging the Euro Banking Association (EBA) Fraud Taxonomy — a common pan-European vocabulary for fraud categorisation — PSPs can ensure their data are not just comparable across the European ecosystem, but also granular and actionable. This paper contends that the move to this pan-European fraud taxonomy will serve as a foundational step in the introduction of fraud data sharing solutions.

Keywords: fraud taxonomy, fraud combating, instant payments, data sharing, IBAN-name check, GDPR, PSD2 review

Annick Moes

Meral Ruesing

INTRODUCTION

In an era where the world of fraud seems to evolve faster than ever, the language we use to describe it is undergoing its own transformation. From trickery to skullduggery, monkey business to jiggery-pokery, the vast lexicon of deceit is not a linguistic curiosity, but a reflection of the complex, ever-evolving nature of deceptive practices used by fraudsters.

The labyrinth of fraud-related language does not end here. Rather, it becomes even harder to navigate if one moves from such high-level descriptions to the granular definitions used by individual payment service providers (PSPs). This is because there has, historically, been no harmonised

Euro Banking Association, 40 rue de Courcelles, F-75008 Paris, France

**Tel: +33 1 53 67 07 00; E-mail: annick.moes@abe-eba.eu*

***Tel: +33 1 53 67 07 00; E-mail: m.ruesing@ebaclearing.eu*

Journal of Payments Strategy & Systems
Vol. 18, No. 1 2024, pp. 61–72

pan-European vocabulary for fraud types. Without a harmonised taxonomy, fraud classifications tend to alter from country to country, and from PSP to PSP — and often, they even differ within organisations. As a result, today's diverse terminology, rather than shedding light on the problem, serves to further obfuscate an already complex dynamic.

The lack of alignment on vocabulary stems from a wider problem faced by the industry: opportunities to join forces have so far been very restricted by a fragmented reporting landscape and regulatory requirements related to data and intelligence sharing. This means that, conceptually, payment fraud has not been a game of cat and mouse, but rather a game of cat and mice, with individual PSPs being pitted against multiple bad actors. This challenge has cut across all aspects of fraud combating — from the data used to detect fraud to the language used to report it or to develop countermeasures.

With pressure mounting for PSPs to develop and provide faster and better fraud prevention and detection tools, there is a need to level the playing field with comprehensive collaboration between PSPs. Using our analogy, the cats should team up to make this a game of cats and mice.

This is made all the harder by the fact that the goalposts continue to shift. As PSPs look to shore up their defences using the latest technologies, increasingly professional fraudsters are using equally sophisticated techniques, such as deepfakes generated using artificial intelligence, to attack.[1] Unlike fraudsters, PSPs — and the anti-fraud measures and insights they look to use — are often limited by the borders within which they operate, the individual fraud-fighting capabilities they have built up and the data sources they have available.

Increasing pan-European cooperation to fight and prevent payment fraud has, therefore, become a key priority among fraud experts, and the calls for fraud data sharing across the industry are becoming louder, both from market participants and European regulators. For such collaboration to succeed — and for the full benefits of shared data to be unlocked — everyone needs to speak the same language.

The Euro Banking Association (EBA) Fraud Taxonomy — a pan-European approach to payment-related fraud type categorisation, developed by the EBA's Expert Group on Payment Fraud-related Topics (EGPF) — can help to make sure this is the case by shining a light in the linguistic labyrinth and ensuring everyone is headed in the right direction.

DEVELOPMENTS IN THE EUROPEAN PAYMENTS LANDSCAPE

The European payments landscape has seen major changes in the last decade — and is rapidly evolving into an increasingly real-time ecosystem. From a standing start, SEPA instant credit transfers (SCT Inst, also commonly referred to as 'instant payments') have gone from 0 per cent of all conventional SEPA credit transfers (SCT) in 2018 to about 14 per cent in Q1 2023.[2] This upwards trajectory shows no sign of abating. For example, the RT1 System, EBA CLEARING's real-time gross settlement system for the execution of SCT Inst, averaged nearly 2.7 million transactions in December 2023, with an average value of €2bn — representing a 35 per cent increase in volume and 100 per cent in value from December 2023.[3]

The continued growth and expansion of instant payments is the result of ongoing regulatory action in Europe, as well as organic growth driven by the opportunity for PSPs and their customers. For the end user — whether a large corporate, small and medium-sized enterprise or consumer — the advent and proliferation of instant payments are bringing the ability to complete time-sensitive payments quickly, wherever and

whenever necessary.[4] The PSPs enabling this trend are equally seeing benefits, such as the ability to maintain competitiveness with new and existing challengers by offering new use cases for customers.[5]

There is, however, a flipside to instant payments. Faster settlement times introduce significant changes to the transaction processing systems of PSPs. Take a traditional payment today: the longer settlement times give PSPs more time to perform the requisite fraud detection and prevention activities. As more transactions are performed instantly, it is necessary for these checks to be performed within seconds. In tandem, the cash-out by fraudsters can take place a few minutes after the transfer because, in the case of instant payments, funds are made available immediately on the beneficiary account.

For those looking to detect and prevent these attacks, it has become a high-stakes race against the clock, as well as an ongoing balancing act between offering fast and seamless services and providing robust and reliable fraud checks. Moreover, managing this complex dynamic will only get more challenging in the years ahead. For example, in France between 2019 and 2020, Banque de France estimated that there was a 65 per cent increase in fraud losses through credit transfers.[6]

To minimise fraud levels and increase the accuracy of anti-financial crime checks — which often lead to false positive hits that can cause unnecessary rejections — there is a continuous need for PSPs to further optimise their internal systems, including by incorporating 24/7 operational real-time monitoring.[7]

Implementing more robust fraud detection tools is already high on the agenda for most PSPs, with considerable investment going into improving internal checks and balances. Though this can bring incremental change, getting ahead of the game is proving difficult. One way to consistently and reliably keep up with fraudsters is having tools facilitating the sharing of fraud data and intelligence that can be deployed seamlessly across borders and different payment instruments. To get to this destination, greater regulatory clarity and a higher degree of standardisation are required to enable further pan-European collaboration between PSPs. Together, these two components could help to make the difference.

A spotlight on payment fraud

Payment fraud is nothing new; it represents a longstanding and significant concern for PSPs and their clients. But what exactly do we mean by payment fraud? The European Banking Authority Reporting Guidelines under PSD2 set out the reporting process for major incidents and breaches that may lead to payment fraud. In line with these guidelines, the following two general definitions have been developed to group the most common approaches to fraud — and have also been incorporated into the EBA Fraud Taxonomy:

- *Unauthorised payment transactions*: Payment transactions made without the authorisation of the payer, 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.[8] An example of this in practice would be 'card lost or stolen'. In this scenario, a customer's payment card, which has been lost or stolen, is used by a fraudster to purchase goods or services.
- *Manipulation of the payer*: 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 PSP, in good faith, to a payment account it believes belongs to a legitimate payee.[9]

An example of this in practice would be 'safe account fraud', whereby a fraudster calls a bank customer purporting to be a representative of the bank. The fraudster tells the customer that the bank has identified several unauthorised transactions, with the aim of manipulating the customer into transferring their funds to a 'safe account'. This account is, in reality, operated by the fraudster and not the customer's bank.

FRAUD INTELLIGENCE AND DATA SHARING: ON THE HORIZON

While the view of an individual PSP is often very rich, it is necessarily limited by the fact that, for most payment transactions, they can only see the incoming or the outgoing leg. This means that PSPs only ever have one half of the story and are in the dark for the other. Fraudsters, on the other hand, usually act across many accounts, institutions and even countries, meaning that many fraud patterns and other anomalies can only be detected at a network level. Although it is a no-brainer, creating a network effect is by no means straightforward.

Today, the sharing of intelligence and data for fraud combating purposes is still hampered by diverging regulations and regulatory interpretation related to data privacy. For example, the General Data Protection Regulation (GDPR) — brought into effect in 2018 — stipulates that the sharing of personal data is only permitted when it meets the 'legal basis' criteria, as outlined in Article 6 of the GDPR.

In the context of the regulation, personal data are defined as 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier'.[10] This means that, in principle, the sharing of a customer's name or international bank account number (IBAN) is under the scope of GDPR and, accordingly, a 'legal basis' must apply for such processing to be lawful.

Recital 47 of the GDPR explicitly mentions that the processing of personal data strictly necessary for the purposes of preventing fraud constitutes a legitimate interest of the data controller concerned. Such legitimate interest may be a valid legal basis for processing provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, as outlined in the regulation.

The challenge for PSPs in the context of fraud is that there remains a lack of clear guidance as to how the 'legitimate interest' should be approached. This has been a significant roadblock in a number of collaborative fraud-fighting initiatives. Adding to the complexities posed by GDPR, bank secrecy legislation and other legal requirements at a country level pose similar challenges — and can often prove more inflexible than GDPR.

Against a backdrop of regulatory obstacles, there is strong support among fraud experts for the sharing of fraud-related intelligence and data. Overcoming these barriers will be a key factor for the success of a comprehensive, collaborative and pan-European fraud intelligence sharing environment. Fortunately, there are several critical developments on this front.

Introducing requirements for instant payments and an EU-wide IBAN-name check

Believing that the uptake of instant payments in Europe was advancing too slowly — with a host of unrealised benefits, lower efficiency levels and a limited choice of means of payment for the payer — the European Commission has adopted a legislative proposal on instant payments, published in October 2022. The aim of the proposal is to 'ensure that instant payments in euro

are affordable, secure, and processed without hindrance across the EU'.[11]

The requirement for all PSPs to send and receive instant payments in Europe — and the associated ramp-up in volume and value — would have significant ramifications on the ability of PSPs to successfully detect and prevent fraud. In view of this, one of the proposal's key requirements is for PSPs to provide a feature that notifies the payer when a discrepancy is found between the recipient's name and the IBAN supplied by the payer for initiating a payment.

As of today, an IBAN-name check does not exist at a pan-European level. Instead, the landscape is made up of individual services within individual communities and countries — often with limited interoperability.[12]

Rolling out a solution across Europe would also come with data-sharing challenges. For example, an IBAN-name check fulfils the criteria of 'personal data' as defined by the GDPR, which means the usage and storage of the data would have to be closely controlled and applied in a consistent manner across Europe.[13]

A recent report, which explored the viability of a pan-European IBAN-name check approach through a series of interviews with market participants, concluded that standardisation and interoperability were key factors in enabling a harmonised and pan-European deployment of IBAN-name check offerings.[14]

In view of these developments, EBA CLEARING launched its Fraud Pattern and Anomaly Detection (FPAD) project at the beginning of 2023, which leverages the company's centralised view on payment data to support RT1 and STEP2 users in their fraud-fighting activities.[15] The broad range of real-time fraud prevention and detection tools that FPAD will cover also includes an IBAN-name check. The central view that EBA CLEARING's retail payment systems can offer, combined with their full SEPA reach, will uncover a rich network picture that will help support users across Europe in their fraud-fighting efforts. As such, deploying this toolset at a pan-European level would be a major step forward for the entire ecosystem — and would dovetail with the introduction of the new regulation on instant payments.

Supporting fraud-fighting through PSD2 review

The second Payment Services Directive (PSD2), adopted in 2015, set out the rules for all retail payments in the EU — euro and non-euro, domestic and cross-border.[16] In the years since its implementation, PSD2 has helped to shape fraud prevention progress through its Europe-wide obligation for PSPs to provide strong customer authentication (SCA), which predominantly supports the mitigation of unauthorised payment transactions.

In the intervening years, however, new types of fraud have also emerged that are not sufficiently addressed by the measures introduced through PSD2. As noted by the European Commission, there has been an uptick in fraud scenarios where a customer will authorise a transaction on the back of manipulative and sophisticated techniques deployed by the fraudster. Examples include the fraudster impersonating the customer's bank using a lookalike telephone number or e-mail address. In such instances, prevention mechanisms under PSD2, such as SCA, have been insufficient to deal with these attacks.[17]

In light of these new and rapidly evolving fraud types, as well as technological developments in banking, such as the growth in instant payments, the European Commission is set to introduce revised rules on payment services, with a core focus on putting in place a more robust, pan-European set of measures to combat and mitigate payment fraud.[18]

As outlined by the European Commission, the new rules for payment services will include:[19]

- an extension to all credit transfers of IBAN-name check verification services — in line with the legislative proposal on instant payments;
- a legal basis for PSPs to share fraud-related information between themselves in full respect of GDPR (via dedicated IT platforms);
- the strengthening of transaction monitoring;
- an obligation by PSPs to carry out education actions to increase awareness of payment fraud; and
- an extension of refund rights of consumers in certain situations.

FRAUD CLASSIFICATION: HOW IT WORKS TODAY

By standardising the use of fraud prevention tools across Europe — as is being attempted with the IBAN-name check mandate — combined with the creation of a legal basis for the sharing of fraud-related information as set forth in the PSD2 review, a route through the complex web of legal roadblocks to data and intelligence sharing for fraud-combating purposes is being identified.

As outlined, however, the law is just one roadblock. Before building effective fraud intelligence sharing infrastructures, the industry must ensure that the right foundations are in place. One of the missing components in this respect is a widely used, common taxonomy for fraud. Without a common language and categorisation approach, the unstandardised and often unstructured data produced — when shared in the future — will not reliably return accurate or actionable insights for fraud prevention and detection purposes. A common vocabulary for fraud types is, therefore, an important prerequisite for sharing fraud data and intelligence between institutions, and while the EBA Fraud Taxonomy meets these needs at a pan-European level, there is a long way to go in terms of adoption.

So, what does the landscape look like today? There is currently a high degree of fragmentation in the way fraud is classified across Europe, with fraud taxonomy approaches created at a regional or national level — such as through local banking or payment associations — or even at individual PSP level. Even where a PSP has a standardised approach to fraud terminology, it can be hamstrung by divergent reporting requirements, including those defined by local or regional authorities, industry bodies or national police forces. These requirements differ in purpose, with the vocabulary shifting depending on the underlying aim. For example, some might be shaped by criminal investigation requirements, while others are focused on cyber security.

As a result, PSPs — particularly those that operate across multiple jurisdictions — end up speaking different languages when referring to fraud. Adding to the complexity, the way payment fraud is categorised and reported is often distinct from the approach for card payment fraud — meaning that the data for each respective area are often siloed within institutions.

This lack of a common classification is not a challenge for PSPs only. It is detrimental at many levels — making cross-border criminal prosecution or cross-industry cooperation on fraud-fighting more complex and difficult to achieve.

These different approaches also negatively impact the quality of data available for fraud-fighting purposes. In practice, the lack of standardisation — both from a language and quality perspective — has become a significant challenge for fraud prevention and detection teams.

A typical example

Picture the scene: a first responder at a subsidiary of a European-wide PSP (subsidiary A) takes a call from a customer who has been the victim of payment

fraud — the details of which are recorded for the purposes of the investigation and internal reporting. The following day, a first responder at a different subsidiary of the PSP (subsidiary B), which is located in a different country, takes a similar call from a different customer who has been tricked by the same technique.

While both responders have been given similar inputs, the output is very different. What the responder in subsidiary A defines as business e-mail compromise, the responder in subsidiary B might categorise more broadly as a phishing attack. This is because at the case management level, both subsidiaries use different taxonomies and the IT systems used to capture the data are not the same. When it comes to feeding the local data into the central reporting tool at the company's headquarters, translation tables are needed to ensure the data are correctly populated.

The different stages of this process take up a significant amount of resources — and instead of discussing the bigger picture that would emerge from consolidating these fraud events and devising potential countermeasures, the teams often lose valuable time by re-discussing individual cases and categorisation options.

STANDARDISATION VIA THE EBA FRAUD TAXONOMY

The existing challenges with how data are recorded at PSPs, combined with the fact that these will likely be compounded in the future as data intelligence sharing matures, have led many payment fraud experts across Europe to recognise the need for greater levels of standardisation in the way fraud is being classified in Europe.

In view of this, the EBA created the EGPF to work towards a collaborative, pan-European approach to combating payment fraud. The objective of the working group was to define the minimum requirements for enabling a fraud-intelligence sharing framework, and to determine what data and information could be exchanged as part of a new, structured approach. To achieve this, the EGPF focused on the fraud type as the most important variable driving the need for specific data input in a fraud-combating context.

Since 2020, the EBA Fraud Taxonomy has offered a standardised way to identify *who* initiated the payment transaction affected by the fraud, *how* the fraudster first contacted the victim and *what* trick the fraudster used to obtain the victim's money or credentials.[20] The EBA Fraud Taxonomy consists of the following four pillars, which make it possible to describe any fraudulent event in a very brief and precise manner:

- *Initiator (who)*: describes who initiates the payment transaction affected by the fraud. Was it the customer or the fraudster? The initiator section also includes 'first party' — in this case, the victim and fraudster are identical — as an optional element relevant mainly to card fraud. The definitions for 'Initiator' within the EBA Fraud Taxonomy are aligned with the European Banking Authority Guidelines on Fraud Reporting under PSD2.
- *Method (how)*: describes the attack vector and specifies the first point of contact between the fraudster and the victim or the point of compromise.
- *Modus (what)*: describes the action taken by the fraudster that resulted in the loss of money via a payment transaction. These actions are clustered within high-level classifications, reflecting the strategic approach deployed by the fraudster. For each modus, a definition is provided based on an authoritative and publicly available source, wherever possible.
- *Labels/tags (PSP individual)*: to ensure ease of use and maximum flexibility, the EBA

Fraud Taxonomy provides the possibility to enrich the case with additional categorisation information on a voluntary basis using labels or tags. The labels/tags listed in the taxonomy are suggestions and not meant to be exhaustive. Individual PSPs remain free to choose labels/tags for specific fraud scenarios as they deem fit, for example to align with internal reporting requirements. For each label/tag, a definition is provided based on an authoritative and publicly available source, wherever possible.

Combining this standardised approach to fraud categorisation with a uniform set of definitions for the different elements, the taxonomy enables the use of a common vocabulary for reporting purposes at a pan-European level and acts as a foundation for fraud intelligence and data sharing across national borders.

Initial implementation initiatives involving the EBA Fraud Taxonomy have been started in different contexts — at an individual PSP, national and regional level — and for different use cases. For example, the EBA Fraud Taxonomy has been used by the European Payments Council's (EPC) Malware Information Sharing Platform (MISP) since April 2022. The latest version of the EBA Fraud Taxonomy — version 4.0 of June 2023 — is available upon request to any interested party.[21]

The how and what: A key differentiator

One aspect that sets the EBA Fraud Taxonomy apart from other approaches is that it distinguishes between the point of contact between fraudster and victim, and the action taken by the fraudster. By comparison, the majority of fraud taxonomies only capture the point of contact indirectly (eg if they classify a trick as 'online shopping fraud') or the categories are too high-level (eg 'social engineering').

By creating separate data points on the 'Method' (how) and the 'Modus' (what), PSPs can leverage higher quality and more granular data in their fight against future fraud attacks. In this sense, capturing the 'Method' is equally, if not more, important than registering the 'Modus'. From the perspective of fraud prevention, the 'Method' used represents an open door through which the fraudster can enter. If the PSP can help identify which door is open, they can inform their customers, who can then close it — shutting the fraudster out.

But how does this work in practice? Table 1 shows the traditional approach versus the EBA Fraud Taxonomy approach. Using a traditional approach, which does not delineate between the 'how' and 'what', a first responder at a PSP might categorise a fraud attack at a high level — in this example, using the terms phishing, smishing or vishing. Using the EBA Fraud Taxonomy approach,

Table 1: The traditional approach versus the EBA Fraud Taxonomy approach

Traditional approach	*EBA Fraud Taxonomy approach*	
No separate categorisation of 'how' and 'what'; no granularity on 'what'	*Separate categorisation of method ('how')*	*Separate categorisation and precise identification of ('what')*
Phishing	E-mail contact	eg Phoney debt/bill collection
Smishing	Text message contact	eg Fake institution
Vishing	Phone contact	eg Safe account fraud

Source: Euro Banking Association

the first responder would be able to separate out the categorisation. When it comes to reporting or sharing the data collected, the traditional approach would produce a single-word description (eg 'smishing'), whereas the EBA Fraud Taxonomy approach would produce a more rounded, precise version of events (eg a fraudster, masquerading as a fake institution, contacted the customer via text). This will increase the likelihood of relevant matches across the network, which, in turn, would allow PSPs to quickly deploy countermeasures that effectively educate or alert customers.

BENEFITS OF THE EBA FRAUD TAXONOMY

Rather than reinvent the wheel, the EGPF has sought to build upon the work already done by fraud experts around the globe. As such, the EBA Fraud Taxonomy relies on definitions from authoritative and publicly available sources wherever possible. For example, in categorising what is meant by payment fraud, the taxonomy leverages the definitions outlined in the European Banking Authority Reporting Guidelines on PSD2 (as discussed in the spotlight on payment fraud).

By introducing a common pan-European vocabulary and approach to fraud categorisation, the EBA Fraud Taxonomy ensures that fraud experts are on the same page — an essential step towards making data comparable between PSPs in Europe and, consequently, facilitating effective data exchanges. This, in turn, will help drive the development of new fraud-fighting strategies at a network level. But the benefits do not end here. The common language has a lot more to offer PSPs, including:

- *Data granularity*: When used to its full extent, some PSPs, which are already leveraging the taxonomy, report getting as many as 45 data points from just eight questions related to a fraud event.
- *Efficiency*: By cutting down on the free-text fields that PSPs currently need to complete, it takes less time to feed cases or transactions into tools, and less time for the tools to process and extract information about cases/transactions. This means the most recent data available can be quickly fed into internal models, which, in turn, will drive improvements in the PSPs' ability to understand and react to fraud. A more rapid turnaround will prove invaluable as the instant payments ecosystem continues to develop.
- *Flexibility*: The taxonomy can be tailored to the specific needs of the PSP — for example, to improve fraud reporting or to develop effective fraud prevention campaigns for customers.
- *A truly European approach*: The taxonomy has been created and developed by more than 30 fraud experts from 15 European countries, many of which represent multinational PSPs. This makes it a truly European product, delivered by the experts on the ground.
- *Regular updates in line with user needs*: Updates to the taxonomy are based on an annual change process to ensure it is future-proofed against evolving fraud trends and upcoming regulations. Any interested party can propose amendments to the taxonomy via the change request form available on the EBA website.
- *Payment and card compatible*: The taxonomy applies to both payment fraud and card fraud, breaking down the siloes that currently exist in the internal and external reporting requirements for these fraud types.
- *Transition friendly*: The ability to use labels supports 'backwards compatibility', which accounts for existing reporting requirements used by PSPs. PSPs can facilitate their transition by using labels to match what is currently in use. This also helps PSPs compare their legacy reports to reports based on the new taxonomy.

- *Enabler of cross-sectoral collaboration*: Clearly identifying the method, ie the point of contact between the fraudster and the victim, can help to inform cross-sectoral cooperation, as this knowledge may help to close fraud entry doors in cooperation with other parties, such as telecommunications or social media providers.

HOW THE TAXONOMY WORKS IN PRACTICE

The EBA Fraud Taxonomy is already proving its value to industry developments. Having a single, common language means that when, for example, fraud experts meet up to discuss incoming regulatory or legislative initiatives, all participants can sing from the same hymn sheet. This, in turn, ensures that less time is taken discussing how to categorise fraud types and more time is spent on value-added discussions to shape the future of fraud detection and prevention.

As mentioned previously, these advantages have been demonstrated in the ongoing discussions on the upcoming legal obligation for PSPs to provide a pan-European IBAN-name check. During these discussions, several open points have come up repeatedly, including, perhaps most pertinently, the question of the actual effectiveness of such solutions for the purpose of combating and preventing payment-related fraud.

To get a clearer picture of the impact an EU-wide IBAN-name check would have on tackling different fraud types, fraud experts from the EGPF used the common terminology of the EBA Fraud Taxonomy to assess the expected impact. Figure 1 gives an overview of fraudulent actions identified as payment fraud 'Modi' by the EBA Fraud Taxonomy (based on the previous version 3.0 of the taxonomy) and evaluates the

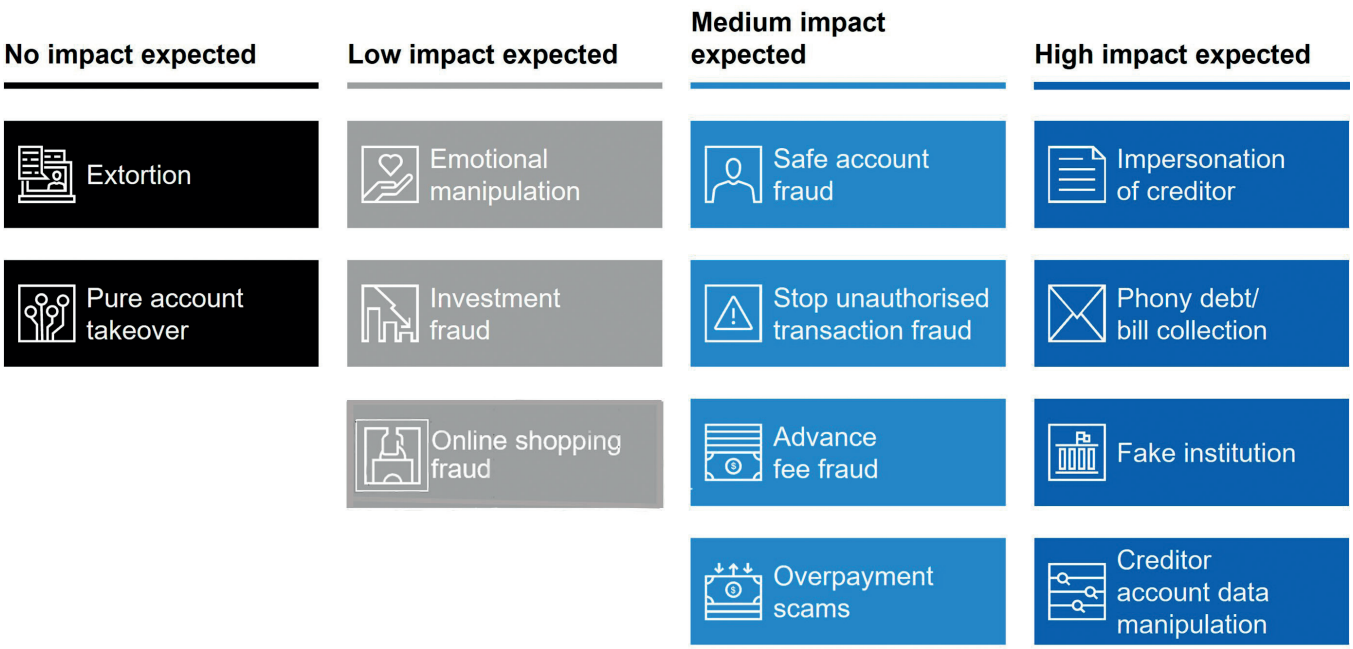

Figure 1: The potential impact of IBAN-name checks on fraud cases for credit transfers

Source: Oesterreichische Nationalbank, Deutsche Bundesbank, Euro Banking Association and Strategy& (2023) 'IBAN-name check: How the rise of instant payments drives IBAN-name checks to prevent fraudulent transactions', available at: https://www.strategyand.pwc.com/de/en/industries/financial-services/iban-name-check (accessed 16th January, 2024).

expected impact of IBAN-name checks on a scale of no impact to high impact.

For example, in a scenario where a fraudster impersonates a known creditor ('impersonation of creditor') or a public authority or institution ('fake institution'), the IBAN-name check — by revealing to the payer that the given account does not belong to the known creditor or institution — will likely have a high impact in preventing fraud. By comparison, in a case of 'emotional manipulation' (eg a romance scam), the payer is more likely to continue believing the fake story told by the fraudster, which will result in a lower expected impact.

While these scenarios are indicative of the anticipated impact of an EU-wide IBAN-name check, fraud scenarios are not black or white — and the actual impact will depend on a range of factors. It is, therefore, important that the IBAN-name check is not treated as the silver bullet, but instead used in conjunction with a wide array of other fraud prevention tools and techniques.

PREPARING FOR TOMORROW'S OPPORTUNITIES

This paper illuminates the reasons for the adoption of a pan-European fraud taxonomy. Having a common language and categorisation approach would help to answer the challenges related to the deep fragmentation in the way fraud types are classified across regions, countries and at individual PSPs, as well as meet the complexities of diverging reporting requirements. In addition, with fraud data and intelligence sharing firmly on the horizon, this effort will act as a key enabler for collaboration on fraud combating.

With this in mind — and in preparation — it is time for PSPs to update their fraud dictionaries. For the era of shared fraud intelligence to be a success, PSPs need to be speaking the same language, such that data can be compared at a pan-European level to provide actionable insights in the fight against fraud. Against this backdrop, the EBA Fraud Taxonomy, which provides a standardised approach to categorising fraud types — with annual updates to fit the changing needs of fraud experts across Europe and beyond — will go from being a 'nice to have', to a 'must have'. To truly capitalise on tomorrow's opportunities, the foundations must be laid today.

REFERENCES

(1) Karim. R (2024) 'Deepfakes: A silent threat to digital integrity and AML efforts', Compliance Week, available at: https://www.complianceweek.com/risk-management/deepfakes-a-silent-threat-to-digital-integrity-and-aml-efforts/34089.article (accessed 16th January, 2024).

(2) European Central Bank (ECB) (2023) 'Work on instant payments in Europe advances', available at: https://www.ecb.europa.eu/paym/intro/news/html/ecb.mipnews230524.en.html (accessed 16th January, 2024).

(3) EBA CLEARING (2023) 'Instant RT1 payments', available at: https://www.ebaclearing.eu/services/rt1/statistics/ (accessed 16th January, 2024).

(4) Bank for International Settlements (BIS) (2016) 'Fast payments — Enhancing the speed and availability of retail payments', available at: https://www.bis.org/cpmi/publ/d154.pdf (accessed 16th January, 2024).

(5) European Payments Council (EPC) (2023) 'SEPA Instant Credit Transfer', available at: https://www.europeanpaymentscouncil.eu/what-we-do/sepa-instant-credit-transfer (accessed 16th January, 2024).

(6) Banque de France (2023) 'Observatory for the security of payment means, annual report 2021', available at: https://www.banque-france.fr/en/publications-and-statistics/publications/observatory-security-payment-means-annual-report-2021 (accessed 16th January, 2024).

(7) European Central Bank (ECB) (2021) 'Benefits of instant payments and recommendations for payment service providers', available at: https://www.ecb.europa.eu/paym/integration/retail/instant_payments/shared/pdf/sept2021_comm_on_instant.pdf (accessed 16th January, 2024).

(8) European Banking Authority (EBA) (2020) 'Guidelines on fraud reporting under PSD2', available at: https://www.eba.europa.eu/guidelines-fraud-reporting-under-psd2 (accessed 16th January, 2024).

(9) *Ibid*.

(10) EU General Data Protection Regulation (2023) 'Art. 4 GDPR Definitions', available at: https://

gdpr-info.eu/art-4-gdpr/ (accessed 16th January, 2024).
(11) European Commission (2022) 'Legislative proposal on instant payments', available at: https://finance.ec.europa.eu/publications/legislative-proposal-instant-payments_en (accessed 16th January, 2024).
(12) Surepay (2024) 'IBAN-Name Check', available at: https://surepay.nl/ (accessed 16th January, 2024).
(13) Oesterreichische Nationalbank, Deutsche Bundesbank, Euro Banking Association and Strategy& (2023) 'IBAN-name check: How the rise of instant payments drives IBAN-name checks to prevent fraudulent transactions', available at: https://www.strategyand.pwc.com/de/en/industries/financial-services/iban-name-check (accessed 16th January, 2024).
(14) *Ibid*.
(15) EBA CLEARING (2023) 'EBA CLEARING to enrich RT1 and STEP2 with fraud prevention and detection capabilities', available at: https://www.ebaclearing.eu/news-and-events/media/press-releases/22-march-2023-eba-clearing-to-enrich-rt1-and-step2-with-fraud-prevention-and-detection-capabilities/ (accessed 16th January, 2024).
(16) European Commission (2023) 'Payment services: Revised rules to improve consumer protection and competition in electronic payments', available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3544 (accessed 16th January, 2024).
(17) *Ibid*.
(18) European Commission (2023) 'Modernising payment services and opening financial services data: New opportunities for consumers and businesses', available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543 (accessed 16th January, 2024).
(19) European Commission (2023) 'Payment services: Revised rules to improve consumer protection and competition in electronic payments', available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3544 (accessed 16th January, 2024).
(20) European Banking Association (EBA) (2024) 'Expert Group on Payment Fraud-related Topics', available at: https://www.abe-eba.eu/market-practices-regulatory-guidance/expert-group-on-payment-fraud-related-topics (accessed 16th January, 2024).
(21) European Banking Association (EBA) (2024) 'EBA Fraud Taxonomy', available at: https://forms.office.com/pages/responsepage.aspx?id=FGYWpwR0NE-UZm-0Sl0jaN0TKDE_8w1CnkPFGgAM58VURUJIWEhDRE1RS0E5NldTOFhRTTJLUTBSTS4u&wdLOR=cB951C75F-46E8-4DE5-8FAD-C2D57B74F8D0 (accessed 16th January, 2024).