September 2024

Report of the ERPB Working Group on fraud related to retail payments

Table of Contents

1. Executive summary: For better consumer protection, we need to boost fraud prevention efforts across the fraud chain

In early 2023, several members of the Euro Retail Payments Board (ERPB) called for the establishment of an ERPB working group related to payment fraud. This initiative was prompted by the rise of fraudulent activities, and the imperative to engage all actors along the fraud chain to enable a more efficient fight against fraud.

As elaborated below, the digitalization of services in recent years, notably accelerated by the COVID-19 pandemic, has introduced increased risks in the form of new kinds of fraud and fraud techniques.

At its May 2023 meeting, the ERPB supported launching a working group on emerging fraud related to retail payments. This working group would analyse developing trends in fraud related to retail payments.

The final report of the working group on fraud related to retail payments (hereafter: the working group) outlines the recommendations formulated by this working group addressed to European Union (EU) and national authorities, as well as to all actors along the 'fraud chain' (please consult Annex V for a list of relevant actors identified by the working group).

Working group discussions have identified issues considered relevant to provisions of the proposal for a Directive on payment services and electronic money services (PSD3)[1] and of the proposal for a Regulation on payment services in the internal market (PSR)[2] currently under consideration by the EU's co-legislators. The working group suggests that these findings are considered by the co-legislators as germane before any finalisation process begins via inter-institutional negotiations.

The working group observed that fraud extends beyond the payment chain. The scope of fraud, its complexities, and the range of actors it involves does not yet fall fully under the mandate of any specific organisation.

To prevent and mitigate fraud more effectively and across the fraud chain, the working group has identified four 'gamechangers'. For each gamechanger, the working group recommends several actions to be implemented by EU and national authorities, as well as institutions and entities from the private sector, as outlined in the table below. Further stakeholder coordination

[1] European Commission's Proposal 2023/0209(COD), for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC, 2023

[2] European Commission's Proposal 2023/0210(COD), for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on payment services in the internal market and amending Regulation (EU) No 1093/2010, 2023

will be required on the timing and content of measures to mitigate fraud through retail payment instruments in parallel to the finalisation of ongoing PSD3/PSR negotiations.

#	Recommended actions	Rationale	Addressees	Deadline
Game changer 1 - Cross sectoral collaboration & responsibilities				
1	Set up an EU network on fraud involving all EU stakeholders identified by the WG, in line with what is also reflected in the current PSD3/PSR negotiations.	Retail payments fraud is a key threat to electronic payments. Fraud prevention initiatives need to mobilize all relevant actors from the local, national and EU level in a collaborative way where stakeholders responsibilities are clearly defined.	ERPB Secretariat coordinating the follow-up actions among relevant EU authorities	Phase 1: Defining the 'who' and the 'why' by June 2025 Phase 2: Setting up of cross sectoral collaboration at EU level by end of Q4 2025
2	Build on the developments of the EU network proposed under Recommended action #1, consider, in the scope of its mandate, possible EFIP follow-up regarding the risks and opportunities of innovation in payments from a payment fraud perspective within EFIP regular work programme by addressing the following questions: - Where can a specific innovation contribute to reducing payment fraud? - Where can an increase of payment fraud be expected due to an innovation in	In today's context of increasing digital payment fraud, there should be no trade-off between innovation and consumer protection.	EFIP[3]	Internal process to address fraud in connection to innovation: in place by June 2025

[3] European Forum for Innovation in Payments

	payments and how can it be mitigated?			
3	Ensure strong coordination between the EPC[4] and the EU cross sectoral cooperation proposed as Action 1	Such coordination is essential to maximize the impact of cross-sectoral efforts and information sharing in compliance with EU data protection and AML/CFT[5] legislation.	EPC	By end of Q4 2025
4	Strengthen existing collaboration or set up new formal or informal cross sectoral operational collaboration focusing on payment fraud and include fraud in their mandate and share views through EFIP on how innovation can help preventing fraud	There is a need to promote and support the exchange of information and share actions implemented against fraud among all relevant national actors identified by the WG.	National Competent Authorities (NCAs) or National Payment Committees (NPCs)	By end Q4 2025
Gamechanger 2 - Sharing Fraud insights & data				
5	Set up an EU wide aggregated data sharing network building on existing networks such as the EPC MISP and connecting all relevant EU and national financial and non-financial stakeholders	To support the cross-sectoral collaboration proposed under Actions 1 and 4, aggregated data should be shared with the communities of stakeholders which can block fraud	ERPB Secretariat coordinating the follow-up actions among relevant EU authorities	Phase 1: defining the 'what' (which aggregated data) by end of Q2 2025 Phase 2; the 'How'; launch of data sharing platform by end of Q4 2025
6	Ensure existing and future national data sharing platforms will be encouraged to connect with the	For the moment there is no EU-wide set of rules and standards for fraud data sharing between PSPs.	EPC	Agree an EU-wide set of rules and standards for data sharing

[4] European Payments Council
[5] Anti-Money Laundering and Countering the Financing of Terrorism

	PSPs[6] community of the EU wide data sharing network, to be able to share and access fraud data available to PSPs in real-time with PSPs across the EU			platforms by end Q4 2025
7	Explore how the governance and technical interconnection capability of the EPC MISP platform could enable fast information sharing about (Indicators of Fraud) IoF beyond PSPs, for instance with Law Enforcement Authorities, Internet Services Providers and Telecommunication Services Providers which can help block fraud	For the moment fast data sharing on IoF beyond PSPs varies across countries and does not involve all relevant internet and telecom services providers.	EPC and EuroISPA[8]	By end of Q4 2025
8	In the framework of EDPB[7] Strategy 2024-2027[9] - Secure cooperation with the relevant regulatory authorities dealing with AML/FTC legislation in line with the Opinion 39/2023 of the EDPS on the proposal for a Payment Services Regulation (paragraph 46-48); - Ensure a coherent interpretation of GDPR[8] rules in the context of payment fraud prevention (e.g., legitimate interest), and an effective enforcement by, and cooperation between, the members of the EDPB	Some fraud prevention measures may be limited to AML/CFT preventing pro-active sharing of fraud suspicion or fraud events. Certain EU and national rules restrict access to and sharing of sensitive data beyond PSPs, notably to protect personal data (GDPR).	EDPB and national data protection supervisors, along with other regulatory authorities on matters with an impact on data protection, including financial regulators.	By end of Q4 2025

[6] Payment Service Providers, in their capacity as providers of payment services as stipulated by Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 25 November 2015
[7] EuroISPA – European Internet Services Providers Association
[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 4 May 2015

Gamechanger 3 - Supervisory enforcement cooperation at EU level across sectors				
9	Clarify within the guidance document on the IPR[9] to allow for cooling off periods for increases in spending limits in IP and include it as a fraud prevention measure in the PSR	Cooling off period for increases in spending limits in IP has proved to be efficient in fraud prevention.	European Commission in the context of the IPR guidance document Co-legislators for changes to the PSR proposal	ASAP and no later than within the agreement on PSR
10	Support cross-sector innovation to prevent fraud by using a more harmonized approach in the GDPR, as mentioned in Gamechanger 2 / recommended action 8	Although the GDPR is an EU regulation, in practice there are differences in its application between data protection authorities. A more harmonized approach for fraud prevention purposes would be desirable. Potential cross-sector innovation for fraud prevention purposes is currently insufficiently supported.	EDPB within the limits of its mandate under Article 70 GDPR	In line with EDPB Work programme 2023/2027 (Guidelines on legitimate interest)
11	Conduct a systematic review of legislation in the field of electronic communication sector in light of fraud risks, such as the ePrivacy Directive[10] and the Network Neutrality Directive[11]	Review of the EU Directives creating clear duties and obligations for telecom providers (ePrivacy Directive and Network Neutrality Directive) is crucial to effectively combat fraudulent activities and protect consumers.	European Commission	As part of the upcoming review of legislation the telecommunicati on sector in 2025

[9] 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, 19 mars 2024

[10] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[11] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code (Recast), 17 December 2018

		Cross-sectoral collaboration is essential, in particular the involvement of the telecommunication providers.		
12	Prioritize contradicting objectives	Engage discussions between the respective European Commission's DGs and with the EDPB. For consumer protection authorities to raise awareness about contradicting objectives, to enhance the development of coherent legislative proposals for fraud prevention and to prioritize in event of contradicting objectives. Legislation should provide a wider mandate for shareholders to prevent fraud, focussed on preventing fraudulent transactions, while balancing consumer convenience, consumers privacy and fraud prevention	European Commission, EDPB and consumer protection authorities	Yearly
13	Foster cross-sector cooperation among competent authorities for the supervision of telecoms, social media platforms and PSPs, data protection authorities, consumer protection authorities and where appropriate law enforcement agencies to enhance a more robust anti-fraud ecosystem in the EU And establish a group to discuss main Modus Operandi (MOs) and fraud prevention	For the moment, knowledge sharing is limited to payment actors. There is a need to create an up-to-date understanding and knowledge of fraud practices to guarantee effective fraud prevention measures and hurdles experience in the market so that the right incentives are applied.	Co-legislators	PSR/PSD3 negotiations

	This group could potentially be established as a community of the EU network on fraud included in Gamechanger 1 / recommended action #1.			
14	Encourage the EBA[12] and the ECB to share rapidly information on fraud trends with the relevant stakeholders identified by the working group (see section 10, Annex V)	Sizing the problem.	EBA and ECB	In line with the data collection under the ECB Payments Statistics Regulation
15	Establish a toolbox of enforcement measures for supervisors	Enhance regulatory convergence across all actors along the fraud chain.	Relevant authorities	PSR/PSD3 negotiations and subsequent implementation and enforcement
16	Ensure incentives for all actors along the fraud chain to invest in fraud prevention	Enhance regulatory convergence across all actors along the fraud chain.	Co-legislators	Include in PSR

[12] European Banking Authority

Gamechanger 4 - Secure Product design for consumer protection				
17	Consider in future legislation regulating new products and techniques including mandatory fraud risk assessments before such products and techniques are launched on the market As regards existing legislation dealing with new products and techniques, a careful fraud risk assessment should be made on a regular basis	Fraud has become a fundamental issue in retail payments because fraud comes from other sectors/actors than the payment actors, which is why we need the European Commission's DGs to work together. To protect consumers against fraud, systematic risk assessments need to be conducted. To avoid that harm is done in the first place, such assessment should be done before a product/technique is launched to the market (by online platforms, telecommunication providers, Internet providers, PSPs). Innovation such as AI[13] and voice recognition are proved to be very efficient tools for fraudsters. Nevertheless, no fraud risk assessments were made for the AI Act[14] and the Digital Services Act (DSA)[15].	European Commissions DG's, in particular DG connect, in consultation with DG FISMA	Ongoing
18	Be more aware of fraud risks, conduct fraud risk training for awareness on their products (for staff as well as customers) and implement fraud mitigation measures (such as	Fraud has become a fundamental issue in retail payments because fraud comes from other sectors/actors than the payment actors. This is why we need all	Market participants (as included in Annex VI, Section 11)	Ongoing

[13] Artificial Intelligence
[14] European Commission's Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, 2021/0106(COD), 2021
[15] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

	those referenced in Annex I, Section 6) for existing as well as new products	actors in the fraud chain to be aware of the fraud risks and to take action before implementation of their new products to avoid misuse by criminals.		

2. Scope definition and methodology of work

As outlined in its mandate (see Section 7. Annex II of this report), the working group on fraud related to retail payments was tasked by the ERPB Board with delivering a mapping of possible actions concerning the prevention, mitigation, and investigation of fraud by different types of stakeholders, as well as complaints to the authorities, in compliance with data protection requirements and based on an analysis of the current state of fraud for retail payment instruments with a focus on new/emerging fraud modus operandi and techniques. In the context of this report, fraud prevention is to be understood as seeking to stop fraud before it happens while fraud mitigation refers to minimising the impact of fraud when it occurs.

The working group commenced its activities in August 2023. It included relevant stakeholders from ERPB members and guest associations, as well as active participants and observers from public authorities such as the European Central Bank (ECB), European national central banks, the European Commission (EC), the European Banking Authority (EBA), Europol, and the European Data Protection Board (EDPB).

In view of the overarching nature of fraud and the multitude of actors in the payment chain, DigitalEurope, DOT Europe, the European Internet Services Providers' Association (EuroISPA), and the European Telecommunications Network operators' association (ETNO) were also invited to join the work as guests, but they did not take part in the work in the end. EuroISPA participated in a meeting of the working group during phase 2.

The work was split in two phases.

Phase 1 occurred from August to December 2023 and focused on delineating the scope[16] and agreeing common terminology, while defining the phases of fraud manifestations and patterns.

[16] The delineation of scope & terminologies were developed using public sources, such as the following list:
- Banco de España, Memoria de supervision 2022, 2023
- Banco de España, Memoria de Reclamaciones 2022, 2023
- Banco de Portugal, Report on payment systems 2022, 2023
- Banque de France, Observatoire de la sécurité des moyens de paiement, Rapport Annuel 2022, 2023
- Euro Banking Association, Fraud Taxonomy, 2023
- European Association for Secure Transactions (EAST) report, shared confidentially with the Working Group
- European Banking Authority, Discussion Paper on the EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry, 2022
- European Banking Authority, EBA Consumer Trends Report 2022/23, 2023
- European Central Bank, Report on card fraud in 2020 and 2021, 2023
- European Data Protection Supervisor, TechDispatch 2/2021 - Card-based Payments, 2021
- European Payments Council, SEPA Credit Transfer, 2023
- European Payments Council, 2022 Payment Threats and Fraud Trends Report, 2022
- Febelfin, Numbers 2022: 'Don't be fooled by a phish', 2023
- Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023

For that purpose, two subgroups were established. Subgroup 1 focused their efforts on assessing the scope of fraud making use of numbers and official data from several countries. Subgroup 2 analysed fraud patterns and manifestations and focused on two fraud manifestations: impersonation scam and investment scam.

The working group presented the interim report to the ERPB plenary in November 2023, where the ERPB agreed that the working group would be prolonged for a second phase to enable more discussions among participants.

Phase 2 occurred from January until June 2024. The main conclusion that emerged from the inaugural meeting of this phase (which was organised in-person in Brussels) was the necessity to implement a shift from the current mitigation and prevention measures against fraud. This agreement among members resulted in the delineation of four gamechangers, as detailed below (see section 5).

Two subgroups were created, each one tasked with discussions on two gamechangers (high-level recommendations that would need to be implemented to fight fraud more effectively). Subgroup 1 focused on Cross sectoral collaboration & responsibilities and Fraud insights & data exchange. Subgroup 2 focused on Supervisory enforcement across Europe and Secure product design for consumer protection. The recommendations agreed upon by the working group, based on discussions in the two subgroups, are detailed in the Executive summary of this report (Section 1).

- Which?, The psychology of scams. Understanding why consumers fall for APP scams
- EMPACT Online Fraud Schemes (OFS) Operational Action (OA) 7.1.

3. Situation: an era of a fraud epidemic

The increased digitalisation of services, which was accelerated by the coronavirus pandemic (COVID-19), offers many opportunities but also comes with increased risks in the form of new kinds of fraud and fraud techniques (e.g., deep fake technology). Society is now always online, interacting with the world through a myriad of platforms. The ease and speed of payments have evolved as well. It is this combination that is leading to new opportunities for all types of users, including those with malicious intent.

In recent years there has been a shift from traditional payment fraud (e.g., skimming) on product level to frauds involving social engineering and identity theft. Therefore, although fraud levels are in decline due to effective interventions (i.e., Strong Customer Authentication (SCA) & risk-based approach), these new forms of fraud are on the rise with higher losses as a result.

Examples of trending forms are bank employee-impersonation fraud, investment fraud, and dating fraud, using whole value chains with multiple parties involved. Many institutions (i.e., Europol[17], Global Anti Scam Alliance[18], European Banking Authority[19], European Payments Council[20]) are now raising the alarm about the scale and projected growth in fraud cases and financial losses to consumers, companies, payment providers and authorities. Additionally, these fraud types also result in lower (digital) self-reliance, perceived safety and trust in society and the digital world.

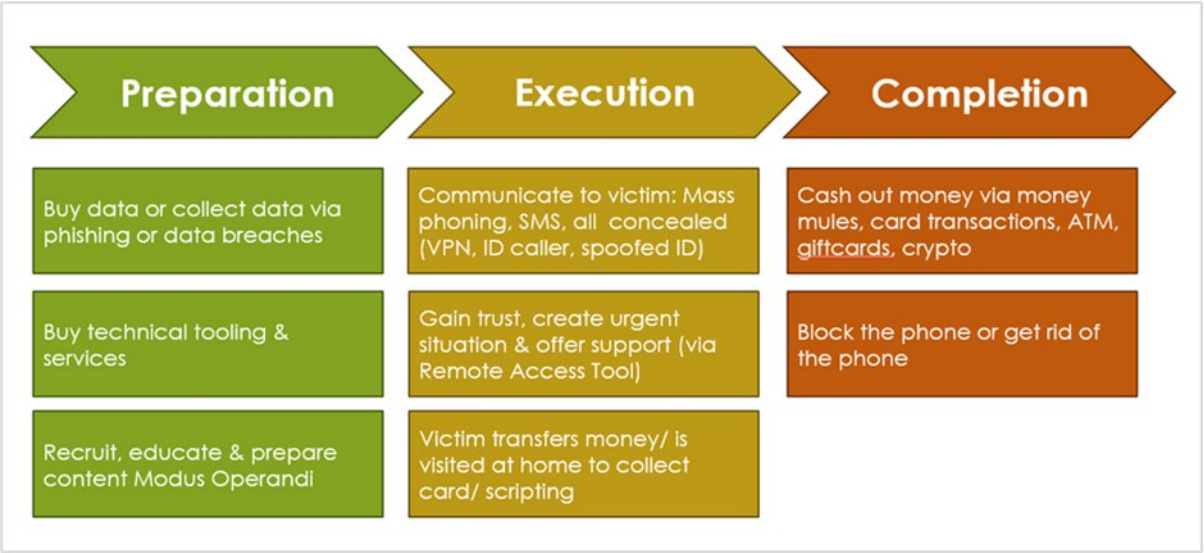
Europol recognizes three phases of an impersonation scam, namely:
1) Preparation;
2) Execution; and
3) Completion.

Per phase different types of tools are used and different actions take place. Per phase different stakeholders are involved. Examples of actions and stakeholders per phase for the specific example fraud form of Impersonation scam are portrayed in figure 1. A more comprehensive overview of observed attack vectors was also brought to the attention of the working group and is publicly available through the MITRE corporation website[21].

[17] Europol, Internet Organized Crime Threat Assessment 2023, 2023
[18] Global Anti Scam Alliance, The Global State of Scams, 2023
[19] European Banking Authority, EBA Consumer Trends Report 2022/23, 2023
[20] European Payments Council, Payment Threats and Fraud Trends Report 2023, 2023
[21] MITRE ATT&CK website, accessed in February 2024

Typically, using electronic communication channels and platforms, criminals will use psychological biases and tactics by creating an overwhelming sense of urgency involving either a too-good-to-be-true opportunity (i.e., investment scam) or threat of potential loss (i.e., bank-employee impersonation scam). Various trusted persons, authorities and institutions are typically impersonated via evolving attack vectors. Using the established trust, they may coach their victims through the payment process, successfully bypassing strong customer authorization protocols. For example, cases of these types of fraud, please refer to section 11, Annex VI.

Figure 1: Criminal actions per phase of scam, example is of Impersonation scam (as explained to the working group by Europol)



4. Complication: Fraud prevention in a challenging environment

The main factors which enable these new types of fraud are the highly complex level and dynamic nature of fraud, which make it difficult to detect for consumers, the ease of onboarding and use of publicly available legal platforms and services with malicious intent (i.e. to create fake merchant or investment websites, spoofed caller-IDs, etc), the low level of security and authentication measures in the new Open Banking context where not only Payment Service Providers (PSPs) are involved but also other actors such as Trust Service Providers (TSPs) and platforms alike (i.e. not properly equipped to avoid theft of personal data and identity theft), the complexity and fragmentation of the payment ecosystem, the cross-border and cross-sector nature of fraud schemes, and the limited cooperation and information sharing among stakeholders.

Although adjustments to the system are made continuously to deter criminals based on known modus operandi (MO), criminals adjust their MO continuously and find ways to bypass the new hurdles. Getting the upper hand therefore requires a real-time 360° view of new threats to enable effective fraud prevention through e.g., pro-active fake account and (merchant-) website take-downs, fraudulent caller ID blocking, and blocking suspected fraudulent transactions. This 360° view is hindered currently by four important hurdles.

1) Fraud cuts through borders and sectors. A 360° view and effectiveness of interventions are therefore dependent on active collaboration, knowledge sharing and timeliness of interventions across all countries and main sectors/players. Even if there are examples of local cross sectoral collaboration, the working group has observed gaps regarding coverage and timely/appropriate action by different countries and sectors. Section 5.1 goes in depth on this hurdle and the proposed Gamechanger: Cross sectoral collaboration & responsibilities.

2) Timely interventions require information to make these types of actions effective. The working group observes that national interpretations of General Data Protection Regulation (GDPR)[22] often do not give room for data sharing for fraud prevention. Due to the large reputational and supervisory risks, actors across the chain fear negative consequences from authorities for sharing relevant information, putting effective fraud prevention interventions on hold. There is also significant variation between GDPR

[22] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

interpretation and domestic data regulatory regimes. This challenges consistent fraud measures across the EU and enables regulatory arbitrage by fraudsters. Section 5.2 discusses the Gamechanger needed to overcome this hurdle: Fraud insights & data exchange.

3) Fraud cuts across sectors and supervisors. The current EU and local supervisory landscape are not organised for such a cross sector-threat. Even in the case that compliance to certain fraud prevention and mitigation falls within one sector, local differences in supervision and action on non-compliance are causing holes in the system that are easily misused by criminals. Section 5.3 covers this hurdle and the proposed Gamechanger: Supervisory enforcement at EU level across sectors.

4) Fraudsters are quick to use new technologies to their benefit, always looking for the weakest link in the chain (i.e., recently, voice recognition, voice cloning). With the current speed of innovation, possibilities created by new technologies such as AI can quickly grow their opportunities and scale. Currently there is insufficient awareness and risk assessment for innovators to ensure their products are not easily misused. Section 5.4 therefore covers this hurdle and the proposed Gamechanger: Secure product design for consumer protection.

5. Gamechangers

A) Gamechanger 1: Cross sectoral collaboration & responsibilities

Further stakeholder coordination will be required on the timing and content of measures to mitigate fraud through retail payment instruments following the finalisation of ongoing PSD3/PSR negotiations.

Situation:

Retail payments fraud is a key threat to electronic payments (and beyond). As stated during phase 1, fraud comes in many different forms, and different stakeholders - including beyond the retail payment chain actors - are involved. To be effective Fraud prevention initiatives need to mobilize all relevant actors from the local, national and EU level in a collaborative way where stakeholders responsibilities are clearly defined.

Complication:

In recent years, there has been an emergence of cross-sectoral collaboration in several Members States, for example via the National Payments Committees (NPCs; in some countries the NPC is called national payment forum) to tackle topics related to frauds.

However, the European Forum for Innovation in Payments (EFIP) 2024 stock-take on national payment committees and national payment strategies results show that cross-sectoral collaboration organized via NPCs varies a lot among Member States, and not all NPCs deal with fraud.

Methodological approach:

Given the limited time available, a non-exhaustive list of existing and missing cross-sectoral areas of collaboration on fraud were identified at local, national and European Union level. The matrix below was developed using the EFIP 2024 Stock take results as starting point and complemented by input from DG CONNECT, EuroISPA and WG members. It helped spot collaboration gaps and identified who could bridge the gaps, helping the WG draft recommended actions for game changer 1.

Figure 2: Matrix of existing and missing cross sectoral collaboration on fraud identified by the WG (Please refer to the enlarged version, including a legend, in Annex II, section 7)

Matrix of existing and missing cross-sectoral collaborations identified

Stakeholders	NCBs via	Supervisors via	PSPs via	Merchants, businesses, national authorities via	Consumers via	Law enforcement authorities via	Telecom providers, via	Social media	Data protection supervisors
European level	ESCB, Eurosystem, EFIP, ERPB (feedback from NPCs)	EBA (ESMA, EIOPA)	ESBG, EBF, EACB, EPC (PSFPWG and PSSG), E-money Association, ETPPA, ERPB	Eurocommerece, e-Commerce Europe, EACT & BusinessEurope, SMEUnited, national public administrations, ERPB	BEUC, AGE, ERPB	Europol (observer in ERPB WG on Fraud)	Digital Europe, DOT, EuroISPA, EuropeanTelecommunicationsNetwork operators' association	GAFA	European Data Protection Board (EDPB)
National level *	National Payments Committees or other cross-sectoral collaboration	National competent authorities identified in game changer #2	National PSPs associtiations	National merchants and e-commerce associations, associations of national/regional public administrations	National consumers/citizens associations	National law enforcement authorities	National telecoms and internet providers, national Digital Services Coordinators (DSA)	national Digital Services Coordinators (DSA)	National data protection supervisors
Local or individual level			PSPs	Merchants, local public authorities	Consumers/citizens	Local police			

** source: EFIP 2024 Stock take results*

Recommendation:

To avoid fraud from spreading the working group recommends the setting-up of a strong cross-sectoral collaboration and timely sharing of relevant fraud data horizontally at EU and national/local levels and vertically between EU and national levels. The cross-sectoral collaboration may even require involving international stakeholders to be effective because fraud is nowadays a serious global threat.

This proposed framework for cross-collaboration on fraud would be supported by Game changer 2 on fraud insights data exchange and game changer 3 on Supervisory enforcement across Europe.

Recommended actions:

At EU level

- Recommended action #1 - **ERPB Secretariat, coordinating the follow-up actions among relevant EU authorities**: Set up an EU network on fraud involving all EU stakeholders identified by the working group. The purpose of this EU multistakeholder collaboration would be to explore how to concretely put in place the cooperation envisaged in the Payment Services Regulation (PSR) legislative proposal with all

relevant financial and non-financial stakeholders such as technical service providers and online platforms, including after fraud has occurred.

- Recommended action #2 **- EFIP**: Build on the developments of the EU network proposed under Recommended action #1, consider, in the scope of its mandate, possible EFIP follow-up regarding the risks and opportunities of innovation in payments from a payment fraud perspective within EFIP regular work programme by addressing the following questions:
    - Where can a specific innovation contribute to reducing payment fraud?
    - Where can an increase of payment fraud be expected due to an innovation in payments and how can it be mitigated?
- Recommended action #3 - **EPC**: Ensure strong coordination between the EPC and the EU cross sectoral cooperation proposed under game changer 1 to maximize impact of cross-sectoral effort and information sharing in compliance with EU data protection and AML/CFT legislation.

At National level

- Recommended action #4 - **National Competent Authorities (NCAs) or NPCs**: Strengthen existing areas of collaboration or set up a cross sectoral operational collaboration (for instance consisting of a dedicated forum or a series of meeting obligations across the different actors involved) focusing on fraud prevention to promote and support the exchange of information and share actions implemented against fraud. They should also include fraud in their mandate and share their views through EFIP on how innovation can help preventing fraud.

All 'fraud chain' actors should be involved in the national cross-sectoral collaboration [23].

[23] The working group recommends that these actors, who are all implicated in the fraud chain, should be involved in a cross sectoral collaboration:

- Consumers via consumer associations
- Merchants
- Businesses
- Public authorities and administrations
- Law enforcement authorities
- Online platforms via the national Digital Services Coordinators recently set up in the supervision framework of the Digital Services Act (Regulation (EU) 2022/2065) (DSA)
- Telecommunication providers
- Internet providers
- Data protection supervisors
- Payment Service Providers, IMEL and IP, TPPs (ASPSP, PISP, AISP)

The enhanced mission of national cross sectoral operational collaboration could include some tasks to be performed, for example:

- Stock-take of existing fraud statistics (e.g., EBA fraud reporting) and analyse specific fraud trends to assess whether current prevention measures applied by stakeholders are still effective or need to be adapted or scaled-up.
- Recommendations to all relevant stakeholders on how to fight against fraud: defining minimum mitigation measures to be adopted by all relevant parties and monitoring the implementation of these measures.
- Technological fraud watch: sharing information on new threats and obstacles in preventing fraud to better fight emerging threats and avoid their spreading to other sectors or countries. Share information with EU level stakeholders to facilitate cross-border sharing.

- Payment Circuits and Card schemes, such as issuers and acquirers
- E-commerce platforms
- Fintechs and/or IT payment service providers
- Qualified Trusted Service Providers and/or Identity Providers
- QTSPs, who provide also TPP compliant eIDAS PSD2 certificates. It is therefore essential that they ensure the correct attribution but also the correct verification over time of their authorization to operate by the NCA
- Hardware manufacturers (smartphones, smartwatches, tablets, etc.) as they rely on their biometric sensors (e.g. fingerprint) or even banks to unlock apps or authorize payments. A certification system for sensors suitable for this purpose could therefore be envisaged.
- O.S. producers of mobile devices as responsible to:
    - the security and integrity of operating systems with respect to external vulnerabilities
    - the functioning/UX of basic services (e.g. SMS messaging which queues SMS or phone calls that appear with the same alias in the same thread despite having different telephone numbers, effectively encouraging spoofing)
    - of the reliability and security of the apps that are uploaded to their respective Stores. The list of malicious apps should be immediately updated and shared and automatically deleted from users' devices with appropriate warning.

B) Gamechanger 2: Sharing Fraud insights & data

Situation:

As stated during phase 1, fraud comes in many different forms and involves different stakeholders - including beyond the retail payment chain actors. Yet collaboration in fraud prevention often only involve payment services providers and law enforcement authorities.

Within the working group on Fraud there is a common understanding that fraud prevention initiatives need to mobilize all relevant actors on local, national and EU level in a collaborative way where stakeholder's responsibilities are clearly defined.

Complication:

No one has the full picture about all elements that could lead to timely fraud detection. However, fraud prevention can become much more effective if a greater amount of information on potentially fraudulent activity is shared with those who can take preventive measures. The framework to enable data sharing on fraud needs to be improved at EU and national levels to involve all relevant actors grouped in communities depending on the level of sensitivity of the shared data.

There are different types of data with different rules applying to data sharing: While it is desirable to share as much information on fraud events as possible (e.g., fraudulent IBANs, location data, behavioural data), some EU and national rules restrict access to and sharing of sensitive data beyond PSPs, notably to protect personal data (GDPR). Some fraud prevention measures may be limited to AML/CFT preventing pro-active sharing of fraud suspicion or fraud events. Yet other actors than PSPs could also play a key role in preventing fraud from spreading to other stakeholders and countries.

New rules apply to technical services providers, but it is too early to assess their impact on fraud prevention: the EU Digital Services Act (DSA) applies to telecom operators and online platforms, which run technical services that are used by fraudsters to operate at large scale and cross-border. Yet they are currently not involved in cross-sectoral collaboration and data sharing on fraud events with payment chain actors, except in a few countries where such collaboration has been set up formally or informally. At EU level, there is no cross-sectoral collaboration between payments chain actors and technical providers.

Methodological approach:

The working group has identified an **example of efficient cross-sectoral collaboration involving a wide range of stakeholders beyond the PSPs: the Italian Financial CERT (CERTFin)**[24].

CERTFin is a public-private cooperative body, established in 2017 and chaired by Banca d'Italia and the Italian Banking Association (ABI). Other Italian financial authorities (Consob and Ivass) are also permanent members while PSPs and operators participate on a voluntary basis. CERTFin's brings together 69 members (Banks/PSPs: 69%, card issuers: 9%, insurance companies: 12%, market infrastructures: 6%, significant providers: 4%) and more than 400 cybersecurity experts related to financial services. CERTFin also works with national and international institutions and organizations (international CERTs, law enforcement authorities, telco providers, etc.).

CERTFin aims at enhancing the cyber resilience of its participants and the Italian financial sector as a whole, by providing qualified cybersecurity services, such as threat intelligence and information sharing on incidents, vulnerabilities, threats and lessons learned, including financial digital frauds. In CERTFin experience, good practices of similar arrangements are:

- The participation of the financial Authorities as trusted third parties (possibly at governance level).
- The use of dedicated and standardised platforms (e.g., MISP) and protocols (e.g. TLP 2.0) to share information within the constituency and with other trusted stakeholders (e.g. cybersecurity, law enforcement agencies, Telco providers).
- Maintaining a comprehensive view on cybersecurity issues by sharing information raised from periodic surveys within the constituency in an aggregated and anonymous way.
- Carrying out coordinated actions to deal with cyber risk and to counter digital frauds.

The CERTFin value added consists of continuous investment, clear objectives and purposes, clear and robust security and privacy policies, and a culture of collaboration and mutual trust.

[24] CERTFin and Banca d'Italia representatives have presented CERTFin's structure and mission to subgroup 1 members on the 11th of April 2024

The working group is proposing to use the effective CERTFin experience in Italy to encourage similar initiatives in other EU member states and to inspire the proposed cross-sectoral collaboration at EU level proposed as game changer 1.

The experience of other successful experiences of data sharing in other countries could also be useful for ex. theNordic Financial Cert which includes members from all five Nordic countries (Denmark, Finland, Iceland, Norway, and Sweden) and in France the ongoing experiment to share fraudulent IBAN.

Recommendation:

Improving consumer protection against new forms of digital fraud requires **new tools and new rules to enable data sharing** of indicators of compromise (IoC) and indicators of fraud (IoF) as well as manipulation techniques and other circumstances associated with fraudulent payments, with all relevant communities of stakeholders gathered in cross-sectoral collaboration against fraud and in line with EU data protection rules.

Shared information should be divided into **three categories** depending on the objective:

- **To prevent fraud: aggregated data should be shared with all actors**: statistical analysis of the most common types of fraud; new types of fraud, methods and techniques used by fraudsters and geographic area where the fraud took place.
- **To block fraudulent transaction in real time: all data relative to a confirmed fraudster account.** When the fraud monitoring mechanisms provide strong evidence of a confirmed fraudster account, all the data necessary to fulfill these purposes such as the unique identifier, name of the legal or physical person, date of birth of physical person, personal identification number or company's number, e-mail, phone number, device,… **should be collected and shared in real-time with all actors who can help block fraud.** Such data sharing must be counterbalanced by creating clear procedures how consumers who were falsely identified as fraudsters (e.g. victims of identity theft) can be released from the accusations and for instance regain access to a bank account.
- **To manage fraud both in real time and in batch (e.g., recovering and reaccrediting of fraudulent funds):** all data related to ascertained fraud should be timely shared in order to avoid that a fraudster can quickly operate at another PSP and therefore perpetuate frauds. Moreover, as ex-post measure, the PSP of the payee shall

be allowed by EU law to debit the funds already credited without the need for account holder consent during the investigation phase and return them to the payer's PSP once the investigation is finalized and the fraud ascertained. This should be done by guaranteeing proper alignment between the PSR and GDPR any striking the right balance between respecting the privacy of the payee and the interest of the payer in obtaining the information-through its PSP-to recover the funds.

It is worth noting that several WG members raised some concerns about Article 83(3) PSR which states: "*Sufficient evidence for sharing unique identifiers shall be assumed when at least two different payment services users have informed that a unique identifier of a payee was used to make a fraudulent credit transfer*." In their view PSPs should be able to exchange information on any fraudulent or suspicious IBAN and/or fraudsters to help other stakeholders detect and prevent fraud. If PSPs have to wait until a second customer reports fraud from a specific IBAN, money mules will move to other PSPs faster, but fraud will persist.

Recommended actions:

- Recommended action #5 - **ERPB Secretariat coordinating the follow-up actions among relevant EU authorities:** Set up an EU wide aggregated data sharing network building on existing networks such as the EPC MISP and connecting all relevant EU and national financial and non-financial stakeholders**.**

This **EU network of networks should be used to share all aggregated information**: statistical analysis of the most common types of fraud; new types of fraud, methods and techniques used by fraudster and the geographic area where the fraud took place. It should also enable real-time sharing of indicators of compromise (IoC), indicators of fraud (IoF), new manipulation techniques and other circumstances associated with fraudulent payments with the communities of stakeholders which can block fraud.

The EU-wide data sharing network should be accessible to consumers organisations, merchants[25] and businesses, public authorities and administrations, law enforcement authorities, payment service providers (ASPSP, PISP, AISP), electronic telecommunication providers, internet providers and online platforms via the national Digital Services Coordinators recently set up in the supervision framework of the Digital Services Act (DSA), with different access rights regarding sensitive data, in line with EU legislation.

[25] Nevertheless, the establishment/operation of a fraud data sharing platform that is accessible to EU PSPs is a non-trivial undertaking that will require significant funding to launch and to operate. It is unlikely that non-PSPs will have full access to any such platform. EU authorities/regulators have rejected previous industry requests to operate such a platform.

A set of rules and standards, including allocation of liabilities associated with the operation of the data sharing network among the above actors distributed according to each specific role within the payment chain, should be defined to encourage a smooth and interoperable implementation of this EU wide data-sharing network in all EU countries.

Finally, this network should properly assess and incorporate data sharing restrictions of the General Data Protection Regulation (GDPR). The reasons are further explained in the opinion of the European Data Protection Supervisor on the proposal for a Payment Services Regulation.[26]

- Recommended action #6 - **European Payments Council (EPC)**: Ensure existing and future national data sharing platforms will be encouraged to connect with the PSPs community of the EU wide data sharing network, to be able to share and access fraud data available to PSPs in real-time with PSPs across the EU.

EPC should also define EU-wide set of rules and standards for data sharing platforms - such as MISP platforms - to encourage a smooth and interoperable implementation of this EU wide data-sharing network for PSP as recommended by EBA in its Opinion (EBA-Op/2024/01) on new types of fraud and possible mitigants (section ‘’Security requirements for a single EU-wide platform for information sharing”, p.13) .

- Recommended action #7 - **EPC and EuroISPA**[27]: Explore how the governance and technical interconnection capability of the EPC MISP platform to enable fast information sharing about IoF beyond PSPs, for instance with Law Enforcement Authorities and Internet Services Providers and Telecommunication Services Providers which can help block fraud.

- Recommended action #8 - **EDPB**: In the framework of EDPB Strategy 2024-2027[28] Pillar 3, **Secure cooperation with the relevant regulatory authorities** dealing with AML/FTC legislation, Digital Services Act, **to ensure a coherent interpretation of GDPR rules in the context of payment fraud prevention** (e.g. legitimate interest),

[26] EDPS: Opinion 39/2023 on the Proposal for a Regulation on payment services in the internal market and the Proposal for a Directive on payment services and electronic money services in the Internal Markehttps://www.edps.europa.eu/system/files/2023-08/2023-0729_d2434_opinion_en.pdf
[27] EuroISPA: pan-European association of European Internet Services Providers Associations
[28] EDPB Strategy 2024-2027 | European Data Protection Board (europa.eu)

and **an effective enforcement** by, and cooperation between, the members of the EDPB (Pillar 2).

C) Gamechanger 3: Supervisory enforcement cooperation at EU level across sectors

Situation:

As stated during phase one of this ERPB working group, fraud goes beyond the payment chain and several stakeholders from different sectors are involved. Social networks are a source of fraud and with their widespread use in society, fraud through social networks is likely to increase. To fight fraud, it is important to involve all stakeholders, and, in this case, social networks must be part of the fight against fraud. To be effective, fraud prevention incentives need to mobilize all relevant actors in the fraud chain and ensure more (regulatory) alignment. This is why the ERPB working group proposes supervisory cooperation between sectors as a gamechanger.

Objective:

Fostering the cross-sector cooperation among competent authorities for the supervision of telecoms, social media platforms and PSP's, data protection authorities, consumer protection authorities and where appropriate law enforcement agencies to enhance a more robust anti-fraud ecosystem in the EU.

Recommendation: Prioritize contradicting objectives

Outcome-oriented fraud prevention obligations:
Fraud is developing fast, and fraudsters constantly adapt their modus operandi. This bears a risk that fraud prevention measures are quickly outdated. At the same time, there are always several objectives which might become contradictory such as privacy versus use of data for fraud prevention. Hence, political guidance on fraud prevention measures remains important to prioritize contradicting objectives.

Systematic review of legislation:
To enhance a more robust anti-fraud ecosystem in the EU, legislation should be systematically reviewed to identify pieces of legislation that need to be reviewed in order to support fraud

prevention and customer protection. See below some examples of existing and sometimes contradicting objectives in EU legislation:

- *Example of the Instant Payment Regulation (IPR)*

The Instant Payment Regulation provides for easy and fast payment. This is efficient for businesses and convenient for consumers but on the other hand it is also efficient and convenient for fraudsters to move money very quickly across countries. This leads to less recovery of money and higher fraud losses. The ERPB WG recommends limit management and a cooling off period for increases in spending limits as best practice of fraud prevention. Conversely, the new IPR states that changing spending limits should be instant. The EC's interpretation of IPR (expressed during last workshop on 30th of April), PSP cannot put limits and PSU should be free to modify his limits in real time without any delay and any other limit by the PSP. Obviously, this is an enormous risk of fraud that will negatively impact both PSP and PSU.

While fraudsters use psychological tactics by creating an overwhelming sense of urgency and coaching customers through the process, one of the most effective fraud prevention measures is to create a cooling off period. This has been proven very effective for instance in the Netherlands where PSP's have implemented a cooling off period of four hours when increasing a (daily) spending limit. Customers can set their limit themselves anytime, lowering a limit is immediate, increasing limit is including cooling off period. In the Netherlands fraud losses related to bank helpdesk fraud declined 45% last year mainly due to these limit measures in combination with awareness campaigns.

- Recommended action #9 – **European Commission**: Clarify within the guidance document on the IPR to allow for cooling off periods for increases in spending limits in IP and include it as a fraud prevention measure in the PSR.

- *Example of the General Data Protection Regulation (GDPR)*

Although the GDPR is an EU regulation, in practice there are differences in its application between data protection authorities. A more harmonized approach for fraud prevention purposes would be desirable. Potential cross-sector innovation for fraud prevention purposes is currently supported insufficiently. Especially, there are more opportunities available for data exchange, not necessarily leading to personal information of the criminal but leading to pause a potential fraudulent transaction, and thus prevent a potential scam. Information that would we valuable for fraud prevention would be for instance the knowledge if a customer is on the

telephone while at the same time doing a transaction (line busy), or using a Remote Access Tool, or contacting a suspicious device/mobile ID number (International Mobile Equipment Identity (IMEI) number). Appropriate EU governance should ensure that fraud considerations are included when interpreting and applying non-fraud specific regulations such as the GDPR.

- Recommended action #10 – **EDPB**: Support cross-sector innovation to prevent fraud by using a more harmonized approach in the GDPR, as mentioned in Gamechanger 1 / recommended action 8.

– *Example of the ePrivacy Directive and Network Neutrality Directive*

The telecoms industry can implement additional safeguards against impersonations fraud, however existing regulation at the EU and national level prevents it from doing so. Should telecoms operators be required to prevent fraud in this manner, work must be done to remove the existing regulatory barriers. Directive 2002/58/EC or the ePrivacy Directive does block telecoms operators from implementing anti- 'spoofing' solutions in most EU member states, by banning the scanning of content of phone calls or SMS messages. In some countries, for example Finland, special provisions have been made by implementing the ePrivacy Directive at national level with allowances for telecoms operators to "undertake necessary measures […] in order to prevent preparation of means of payment fraud", including scanning of calls and messages for this purpose.

A review of the EU Directives creating clear duties and obligations for telecom providers is crucial to effectively combat fraudulent activities and protect consumers. Telecommunications companies should participate in the fight against fraud. The involvement of telecommunications companies should be regulated to provide more tools to help reduce fraud.

Hurdles could be taken away for pattern analysis, blocking of numbers of suspicious devices, investigation and for submitting input for risk engines of PSPs. A series of points that telecommunications companies could address to avoid fraudulent transactions include blocking suspicious devices/phones that have been reported for fraud, being able to validate phones from key business numbers (banking, public administration, etc.), preventing SMS spoofing, prevent receiving international calls with national identifiers.

- Recommended action #11 – **European Commission** Conduct a systematic review of legislation, such as the ePrivacy Directive and Network Neutrality Directive.

- Recommended action #12 – **European Commission**: Prioritize contradicting objectives.

The working group would support a discussion between the respective European Commissions DGs, EDPB and consumer protection authorities to raise awareness about contradicting objectives, to enhance the development of coherent legislative proposals for fraud prevention and to prioritize in case of contradicting objectives. Legislation should provide a wider mandate for shareholders to prevent fraud, focussed on preventing fraudulent transactions, while balancing consumer convenience, consumers' privacy[29] and fraud prevention. The narrow wording/description in legislation currently limits the preventive actions of shareholders as fraudsters are using the latest technologies while adjusting their modus operandi constantly. Hence, certain degree of flexibility to protect consumers is needed within a pan-European regime that ensures sufficient consistency across Member States.

Recommendation: Organize knowledge sharing between supervisors

Situation:

Due to rapidly evolving forms of fraud, adopting regulatory standards does not necessarily equate to sufficient fraud prevention measures. It is crucial for market participants to keep up to date with evolving threats, technologies, and regulatory changes and to adopt fraud prevention measures accordingly. For this there is also a need for PSPs to be able to benchmark against peers and global trends.

Objective:

[29] Recent initiatives aim to begin addressing the balance between privacy and fraud prevention.
Article 94 PSD2 allows payment service providers and payment systems to process personal data when necessary to safeguard the prevention, investigation and detection of payment fraud. PSPs carry out processing of personal data for such purposes under the legitimate interests legal basis under Article 6(1)(f) GDPR. As noted in Opinion 39/2023 of the EDPS (paragraphs 41 and 42), the pending Proposal for a Payment Services Regulation would create a legal obligation in the meaning of Article 6(1)(c) GDPR for PSPs to process personal data for such purposes. The EDPB issued a recommendation in May 2024 aiming to define the limits of such processing of data, with a significant focus on the collection and sharing of personal data that may be relevant for the prevention and detection of fraudulent transactions.
In addition, the EDPB adopted in March 2023 a letter to the European Parliament, the Council, and the European Commission on data sharing for AML/CFT purposes in light of the Council's mandate for negotiations of 28 March 2023 which, while acknowledging that the fight against money laundering and terrorism is an important public interest whose achievement deserves appropriate policies and measures, reiterated the importance to strike a fair balance between this legislative objective and the interests underlying the fundamental rights to privacy and to the protection of personal data. The letter also highlighted that the mere existence of a law introducing (intrusive) sharing of personal data is not sufficient per se and that every limitation to the fundamental rights to privacy and to the protection of personal data must be based on legal provisions that are adequately accessible and foreseeable as to their effect and formulated with sufficient precision to enable any individuals to regulate their conduct accordingly.

Guarantee an up to date understanding and knowledge of fraud practices, effective fraud prevention measures and hurdles experience in the market so that the right incentives are applied to mitigate new fraud types by sharing industry trends, and market best practices regarding fraud prevention and the implementation of standards.

- Recommended action #13 - **Co-legislators**: Foster the cross-sector cooperation among competent authorities for the supervision of telecoms, social media platforms and PSPs, data protection authorities, consumer protection authorities and where appropriate law enforcement agencies to enhance a more robust anti-fraud ecosystem in the EU, we recommend establishes a group to discuss main MOs and fraud prevention measures. This group could potentially be established as a community of the EU network on fraud included in gamechanger 1 / recommendation action #1.

Fraud reporting

Though fraud MO sharing is, in some European countries, handled at national level by banking associations, these initiatives remain very much at country level while there is a perception that a multi-jurisdictional or cross sector supervisory group should be further established at EU level to foster this activity. Nevertheless, changes of fraud MOs cannot be reflected in the reporting requirements on short notice.

Fraud reporting is an obligation for PSPs towards the EBA and the ECB via their respective national central bank (twice per year) and towards the international card schemes monthly. The data is collected and consolidated at EU level by national central banks, and a first high-level summary report was provided to the market[30].

Sizing the problem and benchmark

The benchmarking would require a framework to be able to exchange and share information related to fraud MOs and losses thereof, at national level and international level. This “central” database (of fraud losses and trends) does exist today at the EBA level as PSPs are obliged to report the fraud. Where proportionate to the necessary use of data, relevant data should be made available to market participants.

[30] 2024 Report on Payment Fraud | European Banking Authority and European Central Bank

How information from the EBA database could be shared to the actors of the fraud chain (see section 10. Annex V) for the purpose of enhancing knowledge and fraud prevention to the benefit of the whole ecosystem should be discussed further,

- Recommended action #14 – **EBA**: Rapidly share information on fraud trends with the relevant stakeholders identified by the working group (see section 10, Annex V).

Recommendation: Explore regulatory convergence

- Recommended action #15 – **EBA**: Establish a toolbox of enforcement measures for supervisors.

To ensure that all actors along the fraud chain invest in fraud prevention, and not only some best-in-class actors, more regulatory convergence should also take place, for instance via peer reviews among national competent authorities (NCA's) and having clear requirements on fraud prevention. In addition, NCAs should have appropriate powers to take effective enforcement actions, including the possibility to issue administrative charges in case of violations of regulatory antifraud measures. Beside this, a toolbox of incentives could be explored. It could rely and depend on many factors, such as product and services offered or number and type of customers, which can differ per Member State and could be difficult to compare.

The EBA, in order to reinforce the NCAs activities for fraud prevention measures, should promote the sharing of the most effective fraud prevention practices among authorities in the EU to achieve a high level of standardisation. A level playing field in the EU is welcomed.

- Recommendation #16 **– Co-legislators**: Ensure that incentives for all actors along the fraud chain exist, to encourage these actors to invest in fraud prevention.

Financial incentives are an important driver for implementing fraud prevention measures. Monetary losses should be shared by the different actors in the fraud chain such as PSP's, electronic communication providers and the consumer according to real liabilities. In addition to shared responsibility, including sharing the burden of investments required to better prevent fraud, incentivisation should also be shared. All involved actors should have an incentive to avoid fraud.

D) Gamechanger 4: Secure product design for consumer protection

Situation:

As stated during phase one of this ERPB Working Group, fraud goes beyond the payment chain. Payments are done via technical devices, and several stakeholders from different sectors are involved. Therefore, a multi-dimensional approach should be in place to prevent fraud.

How to guarantee consumer protection when new technologies are being introduced?

Various communication channels and techniques are used to reach out to the victims. These techniques are misused by criminals for impersonation and concealment. Now, fraud mitigation measures are taken after the fraud has occurred. The relevant providers of these products should take more fraud prevention measures (in cooperation with PSPs) before their products or techniques are launched to the market. Consumers are not always aware or able to use the features that already exist to secure the products or devices they use.

Fraud has become a fundamental issue in retail payments because fraud comes from other sectors/actors than the payment actors, which is why we need the European Commission's DGs to work together.

To protect consumers against fraud, systematic risk assessments need to be conducted. To avoid that harm is done in the first place, such assessment should be done before a product/technique is launched to the market (by online platforms, telecommunication providers, Internet providers, PSPs).

Such risk assessments should also take into account other objective such as privacy and accessibility and suggested fraud prevention measures should not disproportionately hinder the fulfilment of these objectives.

There are some examples in the market:

- Generative AI: Deepfake and Voice recognition: no fraud risk assessment

New apps are introduced for deepfake video or voice recognition. A voice can be replicated after 15 seconds of recording. Deepfake video or voice can be used for impersonation fraud.

AI and voice recognition are proved to be very efficient tools for fraudsters. Nevertheless, no fraud risk assessments were made for the AI Act and the Digital Services Act.

It is highly recommended that mitigating measures are taken by the providers to avoid this.

- Email/SMS

Consumers are frequently spammed by fraudulent emails or SMS with links. It is still very hard for consumers to check the email sender, although technical measures are available. The providers of email and SMS should ensure a safe and secure connection and explore further possibilities to prevent fraudulent links be sent. For instance, Safeonweb in Belgium via which consumers can check websites could serve as an example.

Recommended actions:

- Recommended action #17 - **European Commissions DG's, in particular DG connect, in consultation with DG FISMA**: Consider in future legislation regulating new products and techniques including mandatory fraud risk assessments before such products and techniques are launched on the market. As regards existing legislation dealing with new products and techniques, a careful fraud risk assessment should be made on a regular basis.
- Recommended action #18 - **Market participants (as included in Annex VI, Section 11)**: Be more aware of fraud risks, conduct fraud risk training for awareness on their product (for staff as well as customers), and implement fraud mitigation measures (such as those referenced in Annex I, Section 6) for existing as well as for new products.

Based on its analysis, the working group suggests a number of follow-up actions, as outlined in its executive summary and detailed in section 5, "Gamechangers," for the ERPB's consideration.

6. Annex I: Examples of best practices across Europe

Best practices were collected through questionnaires circulated to all working group members toward the end of phase 1 (November-December 2023).

The collected input was classified into prevention and mitigation practices. In a nutshell, fraud prevention seeks to stop fraud before it happens while fraud mitigation seeks to minimise the impact of fraud when it occurs and, in this report, also includes the detection of fraud that could not be prevented at first instance. No best practices were submitted on investigation.

The working group did not evaluate the effectiveness of the collected best practices but rather sees them as examples of measures which public and private actors can use for inspiration in their fight against fraud.

A. Examples of prevention best practices

A.1 Raising awareness of potential fraud risk among bank staff, consumers and merchants

Through campaigns, informative e-mails, SMS messages, videos, posts on banking websites and information provided directly in the payment consumer journey, it is key to raise awareness among customers, merchants and bank employees of new fraudulent content posted online, new fraud trends and patterns, new methods used by fraudsters to steal customers' personal data and security credentials to take control of their accounts and payment apps, etc, to keep them up-to-date and to inform payment service users, what to do to avoid falling victim.

It is also important to continue to regularly inform merchants and consumers about long-existing fraud risks. For ex. remind them that payments through mail and telephone orders (MOTO) can be insecure. In MOTO transactions, the merchant and the customer never see each other in person, so there is a higher risk of criminal activity. There is no record of a PIN number or another kind of evidence with MOTO, so there is no way to ensure the payment is legitimate. Because there is no solid proof linked to the person who approved the payment, it is also more difficult to spot fraud with a MOTO transaction. Merchants and consumers should be reminded that payment methods which require a strong customer authentication are safer to use than MOTO.

A.2 PSP use of machine learning and predictive models to improve fraud prevention

Machine learning can help PSPs detect potentially fraudulent behaviour and transactions by analysing patterns and identifying anomalies in data, enabling them to block suspicious transactions. Then engaging in manual review can help prevent fraudulent transactions by reviewing transactions flagged as suspicious, but this requires extensive manpower.

A PSP's security posture is the collective and comprehensive measure of the security status of all its software, hardware, services, networks, information, third-party vendors, and service providers. It represents the PSP's ability to manage and mitigate cybersecurity risk and is indicative of the effectiveness of the protective mechanisms, policies, procedures, and operations instituted to safeguard its assets. Monitoring security posture can help identify IT or device related vulnerabilities and help detect or prevent fraudulent transactions.

A.3 Preventive measures to lower risk connected to specific scenarios

The introduction of Strong Customer Authentication (SCA) by Article 97 of the Second Payment Services Directive (PSD2)[31] resulted amongst others in eCommerce merchants implementing the fraud prevention protocol, EMV 3DS, which enables consumer authentication for Card Not Present (CNP) purchases and had as part of the SCA implementation a positive impact on fraud containment.[32]

Customizing policies can also help prevent fraudulent transactions by setting rules and restrictions based on user behaviour and by targeting specific product categories, amounts, situations, etc. Examples of customizing measures include:

- Lowering payment limits by adapting them to the consumer's regular uses. Implementing spending limits helps safeguard the banking account associated with the debit or credit card.
- Giving the customer the option to "deactivate/reactivate" contactless payments,
- Giving the customer the option to set up payment alert notifications.
- Allowing consumers to request their PSP to alert them before a transaction to a payee located in another country (especially outside the SEPA) is processed. Such limitation should be designed in a way that protects especially consumers who seldom or never transfer payments to other countries while not hampering consumers form making full use of the European Economic Area (EEA).

[31] Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, 25 November 2015

[32] Banco de España, Memoria de supervisión, 2023, (page 94)

A.4 Introducing regulation targeting actors beyond payment actors to prevent fraud

Regulating telecommunication operators to prevent spoofing scams from fixed numbers and mobile numbers[33] as done for ex. through legislation in France[34] and Spain[35] can be useful to prevent new forms of fraud.

Similarly registering SMS Sender IDs can help prevent SMS message scams, as done in Finland by Traficom, the Finnish transport and communication agency [36].

B. Examples of mitigation best practices

B.1 Awareness raising among bank staff, PSU, merchants and consumers

In the absence of an effective mechanism to prevent social engineering attacks, it is important to continue to inform and educate bank staff, consumers and merchants on existing fraud. Examples of such mitigation measures include regular updates of payments institutions' websites on identified fraud occurrences, explaining how these fraudsters proceeded, and guidance on how PSUs, consumers and merchants can report fraud to their payment institution and seek support.

B.2 Data sharing on detected fraud

Date sharing platforms use fraud detection algorithm (AI) to analyse large datasets from different data streams containing information about transactions. These algorithms are designed to recognize patterns and identify discrepancies that indicate ongoing fraudulent activity. In compliance with personal data protection rues (GDPR) information is shared with platforms members that can take action to block fraud and prevent it from spreading.

[33] "Text message scams done by criminals are becoming more difficult - more than 70 sender IDs are already protected", Tracfin, published on 20 February 2024

[34] Loi n° 2020-901 visant à encadrer le démarchage téléphonique et à lutter contre les appels frauduleux, dite loi Naegelen, 24 July 2020

[35] Real Decreto 381/2015, por el que se establecen medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos en comunicaciones, 14 May 2025

[36] SMS Sender ID", Tracfin, last update on 13 February 2024

The sharing of information can be organised through cross-sector operational organisations involving all relevant stakeholders, as is the case of the French Observatoire de la Sécurité des Moyens de Paiement[37] (OSMP) which seeks to promote the exchange of information and consultation between all parties (consumers, merchants and businesses, public authorities and administrations, payment service providers). Similarly, the Italian Financial CERT (CERTFin) - which inspired Game Changer 2 - is a good example of national cross-sectoral cooperation involving actors beyond the retail payment actors and connecting their network of networks with the EU EPC MISP Platform[38].

Fraud data sharing can also take the form of centralised data sharing platforms or alliance such as Gasa, the Global Anti-Scam Alliance[39]

B.3 Examples of mitigation measures PSPs can put in place

Giving the customer the possibility to quickly revoke a payment means (i.e.: a card or a wallet) at any time can help prevent fraudsters from following fraudulent payments using the compromised payment mean.

Implementing spending limits or adapting already existing limits to the consumer's regular uses helps safeguarding banking accounts and accounts associated with a payment card.
With the entry into force of the Instant Payments Regulation, the IBAN name check is mandatory for both instant and regular credit transfers and thus contributes to the mitigation of such types of fraud, where IBAN and name of the payee do not match. "SEPAMail (Diamond)"[40] in France, Name Check offered by the CBI in Italy, Surepay in the Netherlands and the Confirmation of Payee Scheme in the Nordic countries are PSP services for professionals and companies which allows real-time verification by the payer of the payee's bank account, contributing to the fight against fraud, fake IBANs and identity theft. Additionally, the EPC SEPA-wide VoP scheme represents a collective response to addressing the new IPR requirements.

Diligent use of AI and machine-learning models can also help mitigate fraud. For ex. the use of monitoring mechanisms as required under Art. 2 of the Commission Delegated Regulation

[37] Présentation de l'Observatoire de la sécurité des moyens de paiement (OSMP) | Banque de France (banque-france.fr)
[38] Fraud prevention and payment security | European Payments Council
[39] Protecting Consumers Worldwide from Scams | Global Anti-Scam Alliance (GASA)
[40] SécurIBAN – Professionnels - Crédit Agricole (credit-agricole.fr)

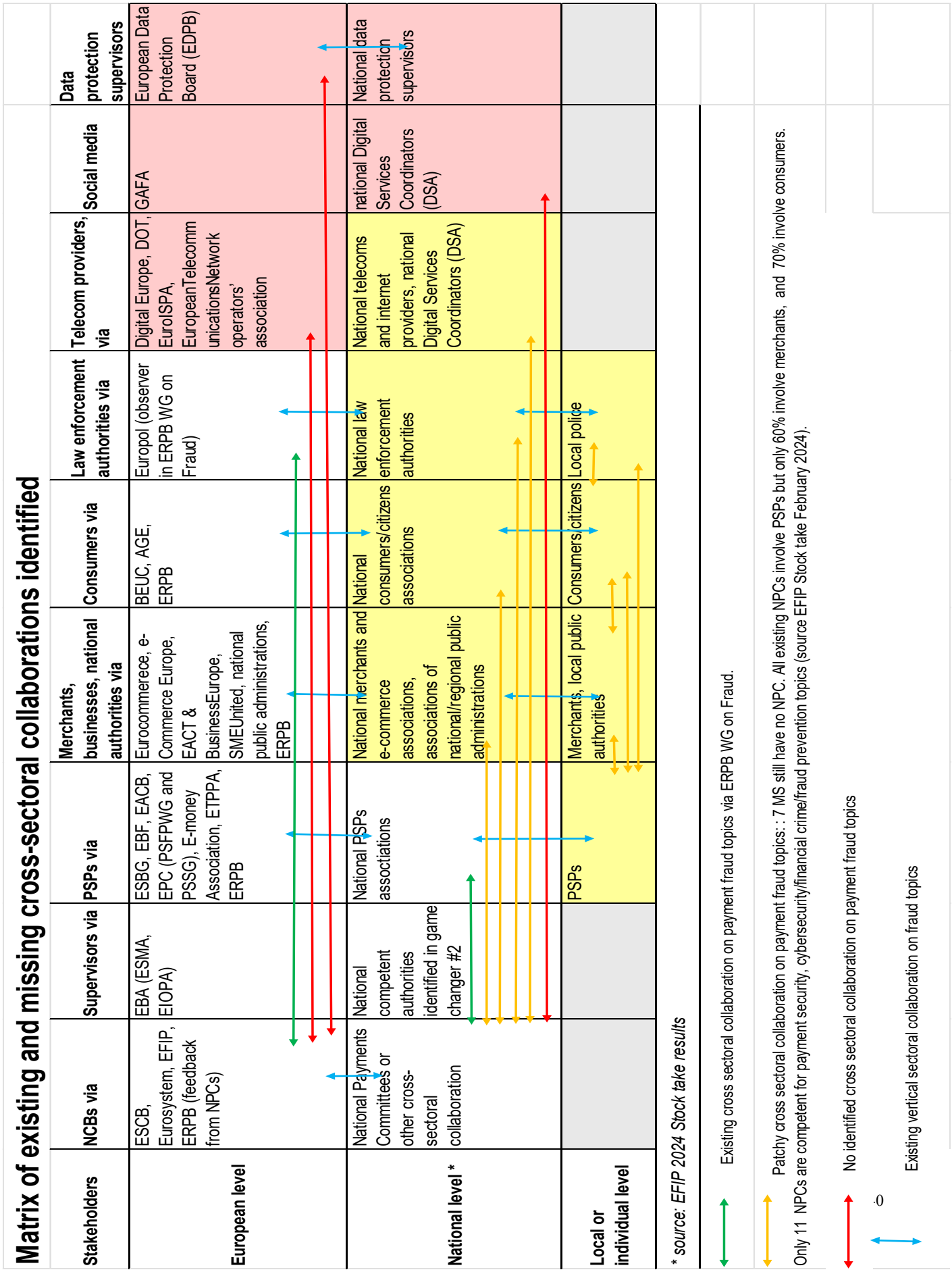
2018/389[41], that are based on behavioural and environmental characteristics related to users' payment habits have proved effective.

In the USA, the Federal Trade Commission in the United States announced that an Impersonation Rule went into effect in April 2024. The rule provides the Agency with stronger tools to combat and deter scammers who impersonate government agencies and businesses through enabling the FTC[42] to file federal court cases seeking to get money back to injured consumers and civil penalties against rule violators. The developments in the USA could serve as a source of inspiration for a similar initiative in the European Union.

[41] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication

[42] Federal Trade Commission | Protecting America's Consumers (ftc.gov)

7. Annex II: Matrix of existing and missing cross sectoral collaboration on fraud identified by the working group



8. Annex III: Mandate of the ERPB Working Group on Fraud related to retail

EUROPEAN CENTRAL BANK
EUROSYSTEM

ERPB Secretariat

ECB-UNRESTRICTED

August 2023

ERPB/2023/011

Mandate of the Working Group on fraud related to retail payments

Based on Article 8 of the mandate of the Euro Retail Payments Board (ERPB), a working group is set up with the participation of relevant stakeholders to analyse developing trends in fraud related to retail payments and define on this basis a set of possible actions for actors involved in the payment chain.

1. Scope

Fraud is a key threat for electronic payments (and beyond) which requires all parties to be aware and contribute to its prevention.

The increased digitalisation of financial services, which was accelerated by the coronavirus pandemic (COVID-19), offers many opportunities but also comes with some increased risk in the form of new kinds of fraud and fraud techniques (e.g. deep fake technology). There has been a shift from traditional payment fraud (i.e. skimming) on product level to types such as social engineering, identity theft and boiler room fraud, using whole value chains with multiple parties involved.

The fight against these new types of fraud faces a number of challenges, such as the fact that the increasing use of digital services comes with a growing fragmentation in payment methods and an increased number of actors in the payment chain. The speed in which payments are being processed and the growing trend for instant payments to become the new normal leave less time for ex-ante fraud prevention measures. Data analysis can support both the detection and prevention of fraud but needs to be balanced against the need for data protection.

In view of these new trends, the working group will analyse the current state of payment fraud in Europe with a focus on the shift in modus operandi/techniques, and develop guidance on effective measures against these new/emerging fraud types. In doing so, the working group will take a cross-sectoral approach, as modus operandi in payment fraud increasingly show multiple online and offline touch-points before paying-out occurs. Specifically, the role of social networks, telecommunication providers and internet providers will need to be included in the analysis.

This work would provide the market perspective on fraud, complementing authorities' efforts to reduce fraud and in particular the ongoing work conducted in the context of the European Forum on the Security of Retail Payments - SecuRe Pay Forum – co-chaired by the ECB and EBA. The ERPB working group will also take stock of the ongoing activities at the EPC Payment Schemes Fraud Prevention Working Group (PSFPWG) and Payment Security Support Group (PSSG)[1], and lessons learned at SEPA community level. The outcome of the ERPB working group's analysis could be channelled to relevant public bodies to inform their work.

2. Deliverables

The working group is expected to deliver a mapping of possible actions concerning the prevention, mitigation and investigation of fraud by different types of stakeholders, in compliance with data protection requirements and based on an analysis of the current state of fraud for retail payment instruments with a focus on new/emerging fraud modus operandi and techniques.

3. Time horizon

The working group will be established in August 2023 and shall present its interim findings by November 2023.

The ERPB will consider next steps on the basis of this presentation.

4. Participants and chairmanship

The working group shall include relevant stakeholders, including representatives of ERPB member and guest associations. Other relevant stakeholders may also be invited to join as relevant third parties. One representative of the ECB and a limited number of representatives of euro area NCBs are invited to join the working group as active participants. A representative of the EU Commission will be invited as observer. Given the scope of work, participants from the European Banking Authority, Europol and the European Data Protection Board would also be invited to join the working group as observers. Their attendance at meetings of the working group does not imply that they agree with the content of the discussions or eventual deliverables

The working group will be co-chaired by the BEUC (demand side) and the European Association of Cooperative Banks (supply side). The Secretariat will be provided by the European Association of Cooperative Banks.

---

[1] E.g. the yearly EPC Payment Threats and Fraud Trends Report, https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2022-12/EPC183-22%20v1.0%202022%20Payments%20Threats%20and%20Fraud%20Trends%20Report.pdf

Members representing their associations and the co-chairs will be appointed by the ERPB Chair based on suggestions from their respective associations. Other participants – after expressing interest to the ERPB secretariat – may be invited by the ERPB Chair to join the group based on consultation with the members of the ERPB.

To progress on its mandate, the working group may interact with additional parties as relevant and in particular stakeholder associations representing platforms, digital actors and telecommunications (e.g. DigitalEurope, the European Digital Media Association, the European Internet Services Providers' Association and the European Telecommunications Network operators' association).

5. Rules of procedure

The mandate of the ERPB defines a broad set of rules for the procedures of its working groups: the working group takes positions on a ¾ majority basis; dissenting opinions are mentioned in any relevant documents prepared by the working group. The members of the group decide on how to organise secretarial support, timing and rules of meetings and communication via written procedure, as well as on the need and format of any interim working documentation produced. Costs related to the operation, meetings, chairmanship and secretariat are carried by the members of the group themselves.

9. Annex IV: List of participants to the ERPB Working Group on fraud related to retail payments

Co-chairs:

EACB (European Association of co-Operative Banks): Sanne van der Neut

BEUC (European Consumer Association): Miryam Vivar Goméz

Secretariat:

EACB (European Association of co-Operative Banks): Rosalie Vuillemot, Farid Aliyev

Members:

- AGE Platform Europe : Anne-Sophie Parent (subgroup chair)
- European Consumer Association (BEUC): Anna Martin, Jacob Ruben Hansen
- European Payments Council (EPC): Patrick Wynant
- European Association of co-Operative Banks (EACB): Olivier Julou (subgroup chair)
- European Savings and Retail Banking Group (ESBG): Birgit Langeder, Fátima Cereijo, Johan van der Sman, Markus Graf-Marschallek, Diederik Bruggink, Douglas Lockhart
- European Banking Federation (EBF): Adine Wempe-Kalff (subgroup chair), Christophe Bonte**,** Alessandra Chiarini
- European Payment Institutions Federation (EPIF): Mafalda Teixeira
- Electric Money association (EMA): Morgane Laigo, Wasan Khalifat, Judith Crawford
- European Third Party Providers Association (ETPPA): Fanny Rodriguez
- European Digital Payments Industry Alliance (EDPIA): Myles Simpson (subgroup chair)
- Eurocommerce: Julien Lenfant

Active participants:

- ECB (European Central Bank): Lorenza Masoero, Viktoria Hindsberg, Sofia Jin
- Banque de France: Marine Soubielle, Sophie Allain des Beauvais, Marc-Antoine Jambu

- Banca d'Italia: Riccardo Cerruti, Emanuele Pimpini
- Banco de Portugal: Tiago Cordeiro
- Deutsche Bundesbank**:** Andrea Friedrich

Observers:

- European Commission (EC): Markus Metschitzer
- European Banking Authority (EBA): Alessandro Campi, Larisa Tugui
- Europol: Tero Toivonen
- European Data Protection Board (EDPB): Peter Kraus, Celie Allagnat

10. Annex V: List of abbreviations

AI: Artificial Intelligence
AISP: Account Information Service Provider
ASPSP: Account Servicing Payment Service Provide
AML/CFT: Anti-Money Laundering / Countering the Financing of Terrorism
DSA: European Union Digital Services Act
EC: European Commission
EP: European Parliament
ESCB: European System of Central Banks
EFIP: European Forum for Innovation in Payments
ESMA: European Securities and Markets Authority
EIOPA: European Insurance and Occupational Pensions Authority
GDPR: European Union General Data Protection Regulation
IBAN: International Bank Account Number
MISP: Malware Information Sharing Platform
MO: Modus Operandi
MOTO: Mail order/telephone order
NCAs: National Competent Authorities
NPC: National Payments Committees
PISP: Payment Initiation Service Provider
SCA: Strong Customer Authentication
TRA: transaction risk analysis
TPP: Third-Party Payment Service Provider
3DS: 3 Domain Secure

11. Annex VI: List of the actors that could be involved in anti-fraud efforts

The working group recommends that these actors, who are all implicated in the fraud chain, should actively participate in anti-fraud efforts:

- Consumers via consumer associations
- Merchants
- Businesses
- Public authorities and administrations, including the EBA, the ECB, the ENISA and equivalent national competent authorities
- Law enforcement authorities' (police, justice etc.)
- Online platforms via the national Digital Services Coordinators recently set up in the supervision framework of the Digital Services Act (Regulation (EU) 2022/2065) (DSA)
- Telecommunication providers
- Internet providers
- Data protection supervisors
- Payment Service Providers, IMEL and IP, TPPs (ASPSP, PISP, AISP)
- Payment Circuits and Card schemes, such as issuers and acquirers
- E-commerce platforms
- Fintechs and/or IT payment service providers
- Qualified Trusted Service Providers and/or Identity Providers
- QTSPs, who provide also TPP compliant eIDAS PSD2 certificates. It is therefore essential that they ensure the correct attribution but also the correct verification over time of their authorization to operate by the NCA.
- Hardware manufacturers (smartphones, smartwatches, tablets, etc.) as they rely on their biometric sensors (e.g., fingerprint) or even banks to unlock apps or authorize payments. A certification system for sensors suitable for this purpose could therefore be envisaged.
- O.S. producers of mobile devices as responsible to:
    - the security and integrity of operating systems with respect to external vulnerabilities
    - the functioning/UX of basic services (e.g., SMS messaging which queues SMS or phone calls that appear with the same alias in the same thread despite having different telephone numbers, effectively encouraging spoofing)
    - of the reliability and security of the apps that are uploaded to their respective Stores. The list of malicious apps should be immediately updated and shared and automatically deleted from users' devices with appropriate warning.

12. Annex VII: Examples of Investment scams and Bank impersonation scams

To provide clarity and better understand the experience of a fraud victim, here are two examples: one of an investment scams and one of a bank impersonation scam.

An example of Investment Scam:

Victim sees an advert on social media for an investment offer that claims high returns on investment. The website linked to the advert looks credible (realistic photos of staff, professional outlook with comments from clients). After first contact, the victim exchanges more information with the website. They decide to invest. After a short amount of time, first returns are received. All seems fine. The “investment manager” contacts the victim with another opportunity that needs quick action. A larger sum is invested because of the trust established with the first investment. After this investment, the website disappears, and no more communication is possible. The victim understands that they have been scammed. They report the scam to the police and the bank, but the money is gone using mule accounts and crypto.

An example of Bank Impersonation Scam:

Victim receives a call from an unknown number. A woman on the phone explains that she is an employee of the victim’s bank and warns them about a scam risk on their bank accounts. The victim is instructed to move their balance to a special bank account that the woman defines as “bank vault account”. After some additional persuasion, the victim moves the money to the given account. The account’s IBAN starts with ‘ES’. The victim firstly has doubts about the transfer, as this seems to be a foreign account. However, the women explains that ‘ES’ stands for Extra Safety. The victim completes the transfer. After being assured that the money is now secure and that they will be contacted again about next steps, the phone call ends. Two hours later, the victim suspects they have been scammed. They report it to the bank and police, but the money is gone using cash withdrawals.