# Public consultation on combatting fraud and counterfeiting of non-cash means of payment

## B. Trends and obstacles

1. To **obtain credentials** to use in fraudulent transactions, the most important means are:

| | Very important | Important | Slightly important | Not important | I don't know |
|---|---|---|---|---|---|
| Data breaches | ◉ | ○ | ○ | ○ | ○ |
| Acquisition on the open web | ○ | ○ | ○ | ○ | ○ |
| Acquisition on the dark web | ○ | ○ | ○ | ○ | ○ |
| Phishing | ○ | ◉ | ○ | ○ | ○ |
| Malware | ○ | ◉ | ○ | ○ | ○ |
| Skimming or shimming | ○ | ○ | ◉ | ○ | ○ |
| Social or behavioural scams (e.g. dating scams, "Nigerian 419" scams, …) | ○ | ◉ | ○ | ○ | ○ |
| Other (please specify below) | ◉ | ○ | ○ | ○ | ○ |

1.1. Please provide here more details (e.g. relative importance) on other **means to obtain credentials** to use in fraudulent transactions, and any other relevant comment (e.g. possible evolution of these trends): 2*000 character(s) maximum*

EPIF welcomes the European Commission's work to update the framework sanctioning criminal activity where non-cash means of payment fraud are concerned. By improving the effectiveness of prosecution of criminal activity where prevention has failed is, this initiative will foster trust and security in the online environment and contribute to the EU's Digital Single Market.

EPIF members would to emphasise the following points:

- Data breaches are the single largest source of stolen financials.
- Following closely behind is malware and phishing.
- Depending on companies' business models, skimming/shimming and social/behavioural scams may or may not be important sources.
- The open and dark web are simply the marketplace where criminals acquire stolen credentials. The source of these stolen financials will be data breaches, or malware, or the other techniques listed. "Acquisition on the open web" and "acquisition on the dark web" should therefore not be placed on the same level as the other items in the list.

2.1. Please provide here more details (e.g. relative importance) on other **means to use stolen credentials** in fraudulent transactions, and any other relevant comment (e.g. possible evolution of these trends): *2000 character(s) maximum*

The relative importance of the means to use stolen credentials in fraudulent transactions depends on the model of the payment service provider affected; EPIF gathers a variety of business models and all of the items listed under question 2 will of differing importance for members.

3. The main **obstacles** that you encounter when **fighting against and investigating** fraud and counterfeiting of non-cash payment fraud are (please choose **up to 5** obstacles and provide details below):

- ☐ National legal framework
- ☑ Legal framework in other EU countries
- ☑ Legal framework in non-EU countries
- ☐ Lack of adequate technology (including investigative tools)
- ☐ Lack of technical expertise
- ☑ Poor public-private cooperation
- ☑ Poor cooperation among public authorities (national and cross border)
- ☐ Poor cooperation among private entities
- ☑ Other (please specify below)

3.1. Please provide here more details on the **obstacles** that you encounter when **fighting against and investigating** non-cash payment fraud, and any other relevant comment: *2000 character(s) maximum*

At the EU level, it would be helpful to:

- Establish common definitions of non-cash means of payment, and the associated offences and penalties, to ensure a common approach across the EU;
- Foster more cooperation and information-sharing in the context of law enforcement investigations, while respecting the Home State Principle – between law enforcement and the industry, and amongst the different public authorities across the EU; indeed the speed of information-sharing between national authorities can be an obstacle to investigations;
- Criminalise the sale of stolen financials and identity theft;
- Streamline legal frameworks across the EU, to avoid situations were an activity is legal in one country, but illegal in another. Importantly, the right balance should be found between regulatory requirements (e.g. data protection) and the legitimate policy concerns that arise in law enforcement investigations.

# C. Legislation

7. Do you think it's necessary to have more similar **definitions of non-cash means of payment** in criminal law across the EU?

- ☐ No, the definition of non-cash means of payment has no impact on my work
- ☐ No, current EU legal instruments already provide a precise definition
- ☐ No (other reason, please specify below)
- ☑ Yes, different definitions across EU Member States hamper cross-border cooperation
- ☐ Yes (other reason, please specify below)

8. Do you think it's necessary to have more coherent **definitions of offences** related to non-cash means of payment across the EU?

- ☐ No, the definitions of offences related to non-cash means of payment have no impact on my work
- ☐ No, current EU legal instruments already provide precise definitions
- ☐ No (other reason, please specify below)
- ☑ Yes, differences in definitions of offences across EU Member States hamper cross-border cooperation
- ☑ Yes, there is a need to better define at EU level some of the currently defined offences (please specify below)
- ☑ Yes, there is a need to criminalize at EU level other offences related to non-cash payment fraud (e.g. identity theft… please specify below)
- ☐ Yes (other reason, please specify below)

8.1. Please provide here more details on other reasons why more coherent **definitions of offences** related to non-cash means of payment are needed or not needed across the EU, and any other relevant comment: *2000 character(s) maximum*

The EU framework should be updated to take account of new types of non-cash payment fraud where cards are not present, e.g. identity theft and the sale of stolen financial information – card credentials of course, but also credentials to access digital wallets, online banking accounts and other dematerialised payment instruments.

9. Do you think it's necessary to have more coherent **level of penalties** for offences related to non-cash means of payment across the EU?

- ☐ No, the level of penalties for offences related to non-cash means of payment has no impact on my work
- ☐ No, current EU legal instruments already provide sufficiently similar levels of penalties
- ☐ No (other reason, please specify below)
- ☑ Yes, different levels of penalties across EU Member States may result in **different prioritisation** of cases at national level, hampering cross-border cooperation
- ☑ Yes, different levels of penalties across EU Member States may create **"safe havens"** for criminals
- ☑ Yes, different levels of penalties across EU Member States may create **insufficient deterrence**
- ☑ Yes, different levels of penalties across EU Member States may create **inadequate protection of consumers** across the EU
- ☐ Yes (other reason, please specify below)

10. Focusing now on the **national level**, do you think it is necessary to modify the **legislation of your country** concerning non-cash means of payment?

- ☐ No, the current national legislation is well adapted to my needs
- ☑ No (other reason, please specify below)
- ☐ Yes, there is a need to adapt the **definitions of non-cash means of payment** (e.g. include new means of payment, make the definitions more precise,… please explain below)
- ☐ Yes, there is a need to adapt the **definitions of offences** related to non-cash means of

payment (e.g. include new criminal acts, make the definitions more precise,…please explain)

- ☐ Yes, there is a need to adapt the **level of penalties** for offences related to non-cash means of payment (e.g. make them higher / lower… please explain)
- ☐ Yes (other reason, please specify below)

10.1. Please provide here more details on other reasons why it is necessary (or not) to **modify the legislation of your country** related to non-cash means of payment, and any other relevant comment: *2000 character(s) maximum*

EPIF members believe that the EU legal framework should be amended to improve coherence and consistence regarding definitions, offences and the level of penalties. It should also be updated to take account of new types of non-cash payment fraud where cards are not present, e.g. identity theft and the sale of stolen financial information. It follows that national legal frameworks will be amended to reflect this change. We therefore see no need for specific national changes. EPIF rather favours an EU approach that would allow for more cross-border coherence in the legal framework and better cooperation amongst Member States. Cybercrime does not stop at national borders – neither should the means to fight and investigate such crime.

## D. Public-private cooperation

The questions in this section look at **examples** of public-private cooperation that you may be aware of and the **obstacles** to create successful public-private cooperation. The final set of questions in this section look at a specific case of public-private cooperation: **reporting** of fraud by private entities to law enforcement.

11. Please indicate established **public-private cooperation mechanisms** that you are aware of to fight against the different types of fraud of non-cash means of payment:

| | Online bank transfer fraud | Card payment fraud | Identity theft | Phishing | Malware | Compromised ATM or point of sale | Other (please specify below) |
|---|---|---|---|---|---|---|---|
| Established network of points of contact | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Virtual platforms for information exchange | ☐ | ☐ | ☐ | ☑ | ☐ | ☐ | ☐ |
| Operational cooperation based on periodical meetings | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Operational cooperation based on ad-hoc meetings | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ |
| Operational cooperation based on secondment of staff | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Strategic cooperation based on periodical meetings | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☑ |
| Strategic cooperation based on ad-hoc meetings | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Strategic cooperation based on secondment of staff | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| Other (please specify below) | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

11.1. Please provide here more details about the **public-private cooperation** you are aware of (e.g. name, location, participating organizations, what makes it successful, etc…): *2000 character(s) maximum*

Examples of public-private cooperation that EPIF members are aware of include:

- InfraGard, a partnership between the FBI and the private sector.
- "Phishing Initiative" is supported by public authorities in France, Luxembourg and Belgium, as well as the private sector. It allows citizens to report to law enforcement the URLs that are implicated in phishing. It is co-funded by the Prevention of and Fight against Crime Programme of the European Union.
- NCFTA is a non-profit corporation involving international law enforcement agencies and the industry.
- "Signal Spam" is a public-private partnership that allows users to report spam to the public authority or the professional that will take the required action. The programme includes companies and French public authorities.

- In order to collectively work to mitigate and prevent fraud, the following consortium and associations are important: Financial Fraud UK (a collective for UK Industry), BBA (a collective for the UK), Merchant Risk Council, Emailage, Ethoca as well as the European work under the EPC.

13. What are the **obstacles for a successful cooperation** (including information sharing) between public authorities (e.g. law enforcement) and private entities that you encounter within your country and when one of the actors is based in another EU country?

| | Within your country | Within the EU |
|---|---|---|
| Legislation | ☐ | ☑ |
| Misalignment of priorities | ☐ | ☐ |
| Lack of trust | ☐ | ☑ |
| Practical/organizational issues (e.g. incompatibility of information systems, internal organizational policies, language barrier, etc… please specify below) | ☐ | ☑ |
| Other (please specify below) | ☐ | ☐ |

13.1. Please provide here more details about the **obstacles for a successful public-private cooperation** indicated above, and any other relevant comment: *2000 character(s) maximum*

EPIF members have identified the following items that hinder a successful cooperation, and especially information sharing, with public authorities:

- The fragmented implementation of EU legislation creates inconsistencies in the definitions and offences, ultimately resulting in different approaches across in Member States;
- The lack of clarity as to what the information companies share with public authorities will be used for, and to whom it might be forwarded creates a lack of trust;
- The difficult balance between regulatory requirements linked to data protection and banking secrecy for instance, and legitimate policy concerns during criminal investigations.

15. If **reporting to law enforcement** of non-cash payment fraud is not compulsory in your country, should it be?

| | Already compulsory | It should be made compulsory |
|---|---|---|
| For citizens | ○ | ○ |
| For financial institutions | ◉ | ○ |
| For others (please specify below) | ○ | ○ |

16. Please indicate the information **currently included** and the information that **should be included** in the reports of non-cash payment fraud to law enforcement:

| | Currently reported | Should be reported |
|---|---|---|
| IBAN of payer/order | ◉ | ○ |
| IBAN of payee/beneficiary | ◉ | ○ |
| Name of payer/order | ◉ | ○ |
| Name of payee/beneficiary | ◉ | ○ |
| Date of fraudulent transaction | ◉ | ○ |
| Time of fraudulent transaction | ◉ | ○ |
| IP address of payer/order | ◉ | ○ |
| Amount of fraudulent transaction | ◉ | ○ |
| Outcome of suspicious wire transfer (OK/blocked) | ◉ | ○ |
| Lost amount | ○ | ○ |
| Retrieved amount | ○ | ○ |
| Credit card PAN | ◉ | ○ |
| Credit card expiration date | ◉ | ○ |
| Credit card owner | ◉ | ○ |
| Fake URLs (phishing) | ◉ | ○ |
| Compromised ATMs or points of sale identifiers | ○ | ○ |
| Other electronic payment systems (PayPal, Neosurf, …) | ◉ | ○ |
| Other (please specify below) | ○ | ○ |