FACTSHEET

It's time to tackle payment fraud at a systemic level

Currently, consumers have to foot the bill for 86% of losses caused by fraudulent credit transfers with an average value of €1,835. Banks refuse reimbursements for authorised transactions and for unauthorised transactions when they consider the consumer "grossly negligent" – leading to almost systematic refusal. This diminishes trust, especially in European payment solutions such as instant payments[1] and the upcoming digital euro which, unlike international card schemes, do not (yet) offer additional refund rights going beyond EU payment services rules.

Consumer testing from BEUC members shows that consumers of all ages and levels of education have difficulties in distinguishing phishing from genuine communication from their banks.[2] This means systemic solutions to prevent fraud are urgently needed.

Are payment service providers already doing as much as they can?

There are strong divergences between payment service providers (PSPs), which clearly shows that fraud prevention can make a difference. Some PSPs receive significantly more fraudulent transactions than others (ranging from just £41 up to £18,550 per £1m of transactions) according to the UK Payment System Regulator).

A study from BEUC's German member vzbv shows several flaws in PSPs' fraud prevention mechanisms. Fraud prevention is time sensitive but when suspecting fraud, consumers can spend hours trying to reach their bank by phone. Some PSPs are simply unreachable for consumers, but also for fraud prevention teams of other PSPs and are not participating in information sharing agreements which is important to block transactions or freeze money on fraudulent accounts.[3]

Effective fraud prevention tools, such as cooling-off periods for spending limits and transaction monitoring, are not systematically employed. vzbv's study reveals cases where up to 43 transactions of €1,000 were made to a bank account in another country without the PSP suspecting fraud. While many consumers never travel or purchase in countries outside Europe or not even beyond their own Member State, risk parameters are not adapted to the consumer profile which allows fraudsters to send money abroad within seconds.

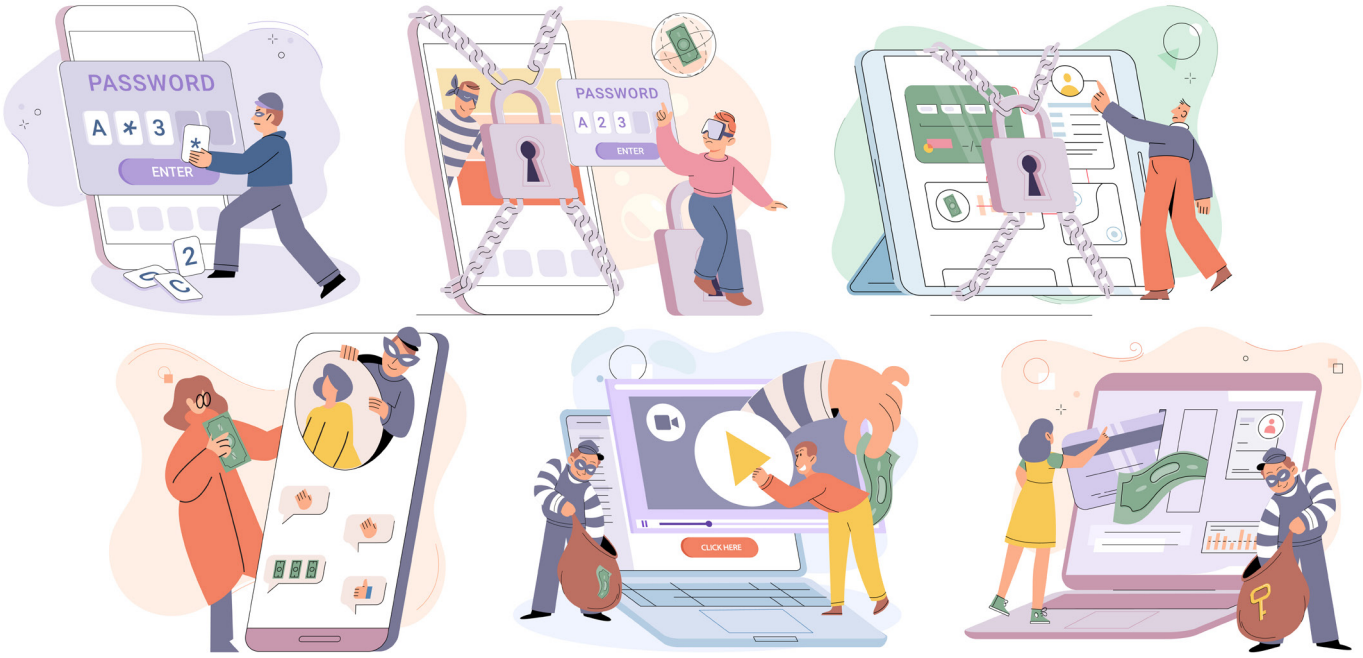
BEUC recommendations:

- PSPs need to be financially liable for fraud losses to give them clear incentives to invest in fraud prevention. Liabilities should be fairly shared between the sending and receiving PSP to foster cooperation between both.
- PSPs should have a clear mandate to block transactions where fraud is suspected and be able to freeze the funds until they can be returned to the fraud victim.
- PSPs need clear obligations to participate in information sharing agreements, being contactable for consumers and other PSPs and to invest in transaction monitoring. PSPs should report fraud figures to national and European supervisors to allow for market supervision and interventions.

[1] Instant payments are used for example by wero, MBWay, Bizum
[2] Consumer testing from vzbv, Consumentenbond and report on in-depth interviews with fraud victims by Which?
[3] For example, European Payment Council "Malware Information Sharing Platform"

BEUC The European Consumer Organisation

Co-funded by the European Union



Why are online platforms and search engines advertising fake shops?

Fraudulent shops and investment ads, and fake comparison tools are being increasingly promoted by online platforms and search engines (e.g. sponsored ads/content). This causes problems for consumers but also reliable merchants online.

Online platforms and search engines can clearly do more to remove fraudulent content. A European Commission dashboard shows that online platforms and search engines remove only a very small amount of illegal content, especially when it comes to fraud. What's more, platforms mainly just delete individual posts instead of suspending or freezing fraudulent accounts.

BEUC member Which? built its own AI tool to test whether platforms could use algorithms to remove fraudulent content. The tool has been tested with the Meta Ad library and proved very successful. If a consumer organisation can build such a tool, why are platforms and search engines not doing it?

Telecom providers play a role in preventing techniques such as spoofing and phishing attacks via telephone, SMS and email. By establishing sound filter systems and ensuring that telephone numbers cannot be spoofed and disabling links in SMS, the number of fraud attacks will decrease.[4]

BEUC recommendations

- Allow PSPs to claim back fraud losses to online platforms and search engines to incentivise fraud prevention along the full fraud chain.
- Payment fraud should be defined as a systemic risk under the Payment Services Regulation to trigger prevention obligations for systemic risks under Article 34 and 35 of the Digital Services Act.
- Replicate effective national measures which allow telecom providers to prevent spoofing and sharing of fraudulent links by SMS.

[4] See for example rules in the French law: Loi pour Sécuriser et Réguler l'Espace Numérique will block all fraudulent links sent by SMS and Loi Naegelen (Loi 2020-901) will instaure a number authentication mechanism as of October 2024 to prevent spoofing.