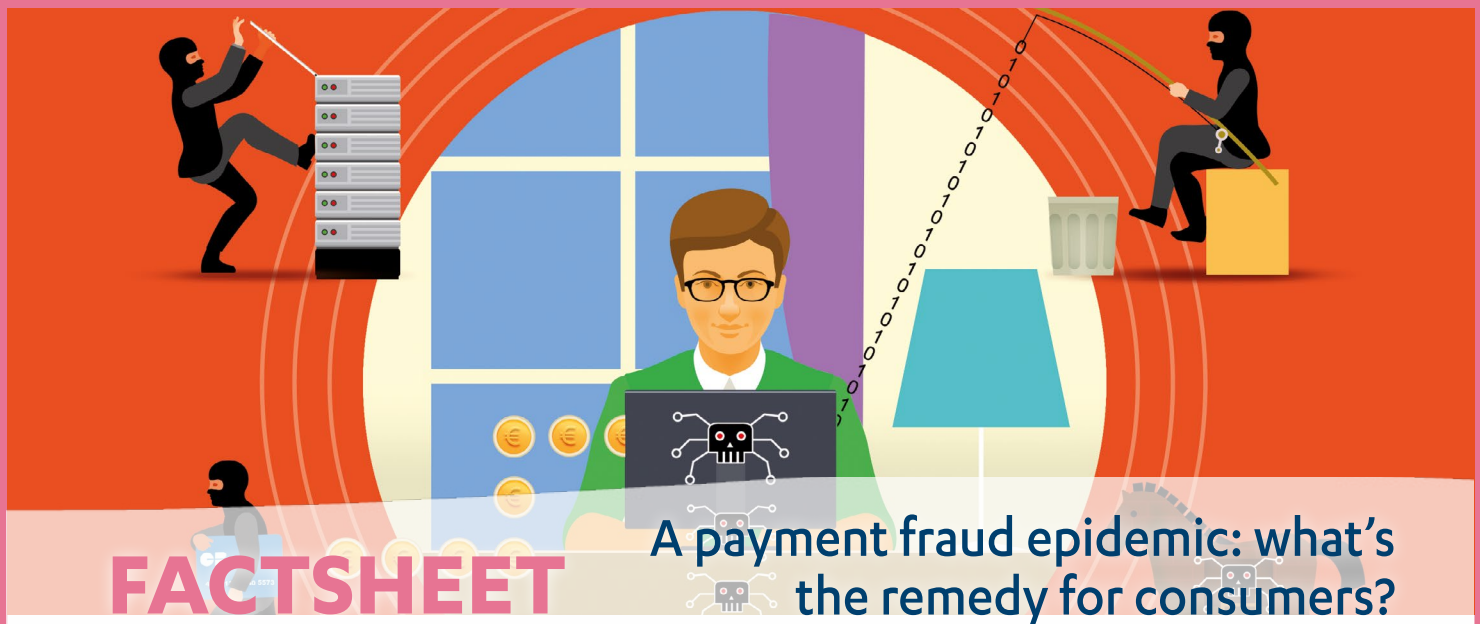


FACTSHEET

A payment fraud epidemic: what's the remedy for consumers?

What is going on?

Nowadays, bank robberies have become rare, as digitalisation allows for much easier ways to steel consumers' money. Today, payment fraud mostly takes place online: data-stealing software is used to access banking data or consumers are tricked into sending money to fraudulent beneficiaries.

Data from the EBA draws an alarming picture: consumers lose €4,191 on average for fraudulent credit transfers. While strong customer authentication made it more difficult to use stolen cards, credit transfer fraud is rapidly increasing: in Belgium, consumers lost €34m in phishing scams in 2020, up from €7.5m in 2019. In the UK, authorised push payment scams increased from €420.7m in 2020 to €573.2m in 2021.

How are fraudsters taking advantage of consumers? Two case studies:

Spoofing

Fraudsters pretend to be a bank representative using the bank's official telephone number or by hacking the social media account of a consumer's contact. Consumers are urged to send money to the fraudster's account to "secure their money" or "to help their friend pay a bill". Victims are often accused of having acted with gross negligence as reported by our members UFC-Que Choisir (France), vzbv (Germany) and the Norwegian Consumer Council. Banks could effectively prevent spoofing calls but often do not take action as reported by Which? in the UK.

Open banking vs. fake websites

Fraudsters send consumers phishing e-mails/SMS with links installing malware or redirecting consumers to fake websites where they are asked to enter their bank credentials, as explained by our Belgian member Testachats.

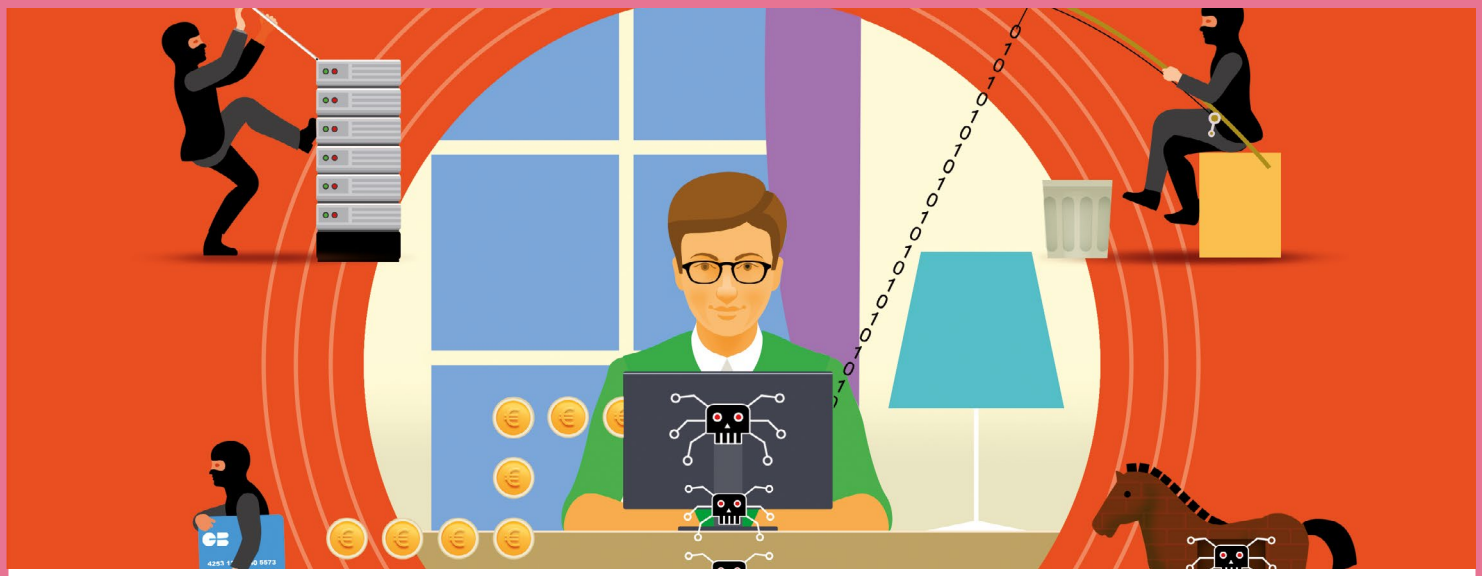
Fake websites are getting more professional and harder to identify. At the same time, consumers are often asked to enter their bank credentials on third-party websites when using open banking (e.g. budget monitoring apps), as vzbv discovered. In some cases, fraudsters even manage to copy banking data when consumers enter it on a non-fraudulent e-commerce website ('formjacking'), as UFC-Que Choisir reported.

What happens when the money is gone?

Consumers bear 68% of the losses according to EBA data: consumers are not reimbursed when they supposedly authorised the payment or when they acted with "**gross negligence**". This leaves a lot of room for interpretation for banks who often treat a transaction as **authorised** as soon as the consumer used strong customer **authentication**. The Polish consumer protection authority UOKiK and the Norwegian Consumer Ombudsman have recently criticised banks for wrongly interpreting the Payment Services Directive 2 and denying consumers reimbursement.

BEUC The European Consumer Organisation

Co-funded by the European Union



Will consumers act carelessly if they are more systematically reimbursed?

No consumer wants to be a victim of fraud. And there is evidence for it: UK bank TSB systematically reimbursed consumers and reported lower fraud losses than the industry's average as they focus more on fraud prevention. Card companies also reimburse consumers more systematically for fraudulent payments via chargeback mechanisms. The temporary loss of money, no matter the final outcome, will create stress and administrative hassle, as Which? discovered.

What does BEUC recommend?

To fight payment fraud, more effective **fraud prevention measures** are needed. BEUC members already share tips and tricks with consumers to avoid common traps. But additional measures are needed:

- A verification of whether there is a mismatch between the IBAN and the name of the beneficiary (**IBAN check**) for all credit transfers,
- **Improved transaction monitoring** and clearly allowing banks to block potentially fraudulent transactions,
- **Involvement of all actors along the chain:** the UK's communication regulator set up measures to prevent telephone spoofing with official numbers e.g. avoiding that a fraudster can pretend being the fraud helpdesk of a bank. Social media platforms could be held responsible for sponsored ads promoting fake shops.
- **Systematic identification of fake websites and scams** and cooperation with all relevant actors as done by the Danish Consumer Council and the Austrian Watchlist Internet, and
- **Give consumers more control:** they should be allowed to quickly and easily block transfers/payment instruments and set transaction limits for their bank accounts which are more difficult to overrule than is the case today

To incentivise fraud prevention and ensure victims are treated fairly, consumers should be **reimbursed more systematically** in case of fraud:

- **Immediate compensation** for unauthorised transactions with gross negligence applying only in exceptional cases. Transactions must be treated as 'unauthorised' if the consumer was tricked into them.
- The **burden of proof** must be on the payment service provider (PSP) not the consumer, and
- **Shared liability between the sending and receiving PSP** so that both PSPs have an incentive to resolve fraud cases.

An improved liability regime must be paired with **better enforcement** mechanisms:

- Obligation for PSPs to inform consumers about their **rights and the procedures to contest a negative decision on reimbursement**,
- Obligation for PSPs to participate in **alternative dispute resolution** and to accept the outcome,
- **Improved fraud reporting** allowing regulators to effectively supervise market compliance. As shown by the EBA, currently only 14 EEA countries report data with sufficient quality,
- **Effective penalties** for banks not reimbursing consumers in due time, and
- **Enforcement powers for competent authorities** to allow for effective structural enforcement.