skillcast

Social Engineering and Fraud Risk

What do financial services firms in the EU need to know?

Financial fraud is on the rise in Europe. According to recent figures, fraud losses reached €4.2 billion in 2024 – a 17% increase from a year earlier – with the EU's largest economies (Germany, Italy and France) recording the highest volume of illicit financial flows.

€4.2
billon in fraud losses during 2024

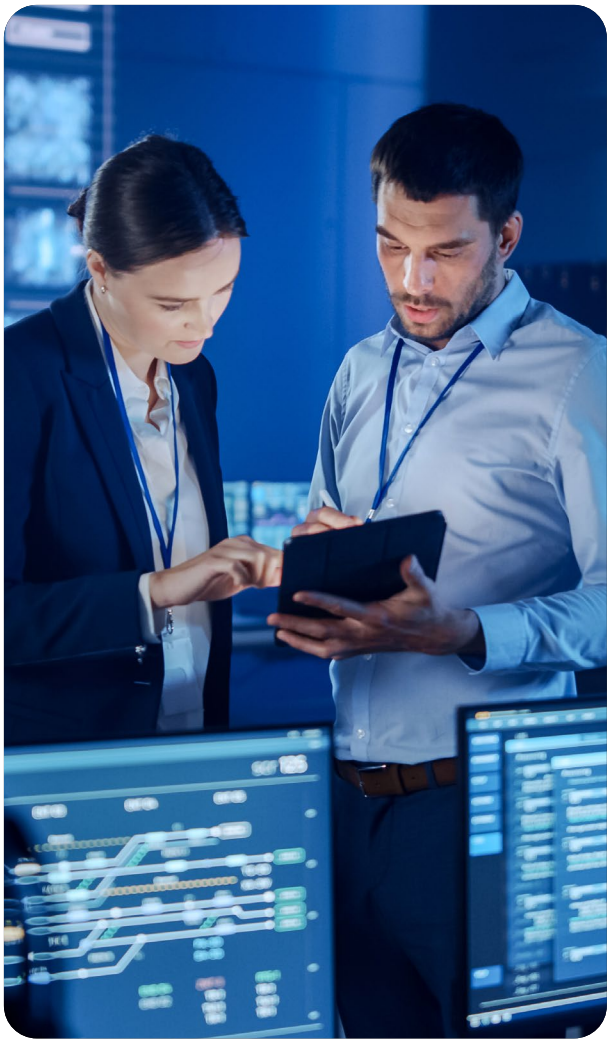
17%
increase from last year

At the heart of this shift is the proliferation of social engineering scams, where criminals manipulate customers or employees into authorising payments, sharing login credentials, or revealing personal data.

This is not a new tactic, of course. But as firms have tightened their cyber defences, fraudsters are increasingly working in the realm of human psychology – manipulating our trust in authority to undermine our ability to spot a scam.

Powerful AI tools have added fuel to this fire, allowing more criminals to execute sophisticated attacks at scale.In this guide, we'll explore the complex tactics fraudsters are using in 2026 and how regulators, compliance teams, and financial firms can adapt.

The rise of social engineering fraud



For financial firms, fraud prevention used to be about securing the perimeters. Banks made their systems as robust as possible with firewalls, encryption processes, and algorithms to spot anomalies in their data. They also implemented strict customer identification checks to detect fraudsters.

But criminal networks have responded by shifting their strategy upstream. While direct assaults are by no means a thing of the past, fraudsters target people rather than institutions because they can be manipulated, especially if they're vulnerable. Using an elaborate array of confidence tricks, they turn customers and employees into unwitting accomplices to financial crime that impacts individuals as well as institutions in the form of fines, reputational damage and low customer confidence.

This is social engineering – a psychological criminal tactic that takes many forms:

- **Enriched impersonation:** Using leaked personal data (such as addresses, birth dates or recent transactions) to appear authentic, tricking victims into transferring money or handing over information.
- **False expertise:** Adopting a professional, knowledgeable tone to mirror the experience of a genuine bank support call.
- **Tactical mimicry:** Using scripts that mimic a bank's safety advice (e.g. "We will never ask for your password") and cloning legitimate bank numbers.
- **Micro-fraud:** Executing minor, repetitive data breaches or small unauthorised transactions to desensitise a target or test their defences.
- **Fraudulent customer support:** Using a fake security notification and a fraudulent number to prompt victims to move money to a supposedly safe account.

I caused the company to be defrauded by scaring the victims into believing there was some sort of virus on their system … They weren't vulnerable, I created a vulnerability.

*- **Alex Wood,** reformed fraudster, now government adviser. Speaking at Skillcast's Compliance and Culture Seminar, Autumn 2025*

Recent figures suggest these methods are only becoming more effective. In 2024, fraud linked to credit transfers rose to €2.5 billion in the EU, with more than half of these cases involving direct victim manipulation.

It's not just customers who are at risk, either – nearly two-thirds of business leaders in a recent UK study expressed concern that their employees would be targeted by fraudsters too. High-profile cases of accidental or intentional employee fraud are becoming more common, placing pressure on firms to train staff effectively to spot the signs of fraudulent activity.

AI and automated social engineering

Artificial intelligence (AI) has made social engineering scams far easier to commit.

Using only a few seconds of recorded video or audio, fraudsters can now create deepfakes that are indistinguishable from senior managers or trusted colleagues. In Hong Kong, a finance worker was tricked into paying $25 million dollars to fraudsters who impersonated his company's chief financial officer.

In the past, awkward phrasing or poor grammar made fraudulent messages easy to spot. Large Language Models (LLMs) like ChatGPT can now produce grammatically perfect emails in every EU language, translate scams into local dialects, and mimic the specific corporate tone of a target firm.

Criminal groups are also building and selling "fraud kits" with the help of AI, featuring tailored scripts, leaked data and laundering pathways. This has lowered the barrier for entry for attacking financial institutions.

This level of deception creates a new challenge for firms. Most banks already have mandatory checks in place – such as fraud checklists to confirm payments on mobile banking apps – but when an attacker uses a perfectly cloned voice or familiar face, victims are far more likely to ignore these kinds of prompts.

> We no longer really need complex skills or techniques to carry out devastating frauds … Criminals can very quickly develop an LLM (Large Language Model), then train it on thousands and thousands of fraud scripts to come up with the perfect fraud.

*- **Alex Wood,** reformed fraudster, now government adviser. Speaking at Skillcast's Compliance and Culture Seminar, Autumn 2025*

Firms will now need to equip staff at every level – from the developers who design banking apps to customer service teams on the phone – to spot the subtle psychological cues that generic prompts and filters often miss.

How does social engineering affect financial firms?

While fraud has now become the second most significant operational risk for European banks – surpassing traditional legal and conduct concerns – the damage caused by social engineering scams extends far beyond immediate financial loss.

As well as regulatory fines, customers who fall victim to fraud, or see reports about it, will likely lose trust in their bank's ability to protect them, and may move to competitors.

Those who lack digital skills or confidence may stop using online banking services entirely.This is not to mention the ethical and human cost of fraud. Victims often suffer from lasting psychological harm after being targeted, including the effects of anxiety, social withdrawal, and depression.

Financial institutions in the EU reported spending €6.5 billion to defend themselves against AI-enabled attacks and data breaches in 2024, suggesting that fraud prevention is now a core operational priority.

With AI-generated scripts and deepfakes making it nearly impossible to distinguish between genuine and fake threats, financial firms will need to work harder than ever to protect their customers' money, confidence and their own reputation.

€6.5 billion

spent by financial institutions to protect against AI-enabled attacks and data breaches in 2024.

How EU regulations are shifting responsibility onto the institution

The current legal framework often excludes financial institutions from liability when a customer authorises a transaction, even when that authorisation was obtained deceptively.

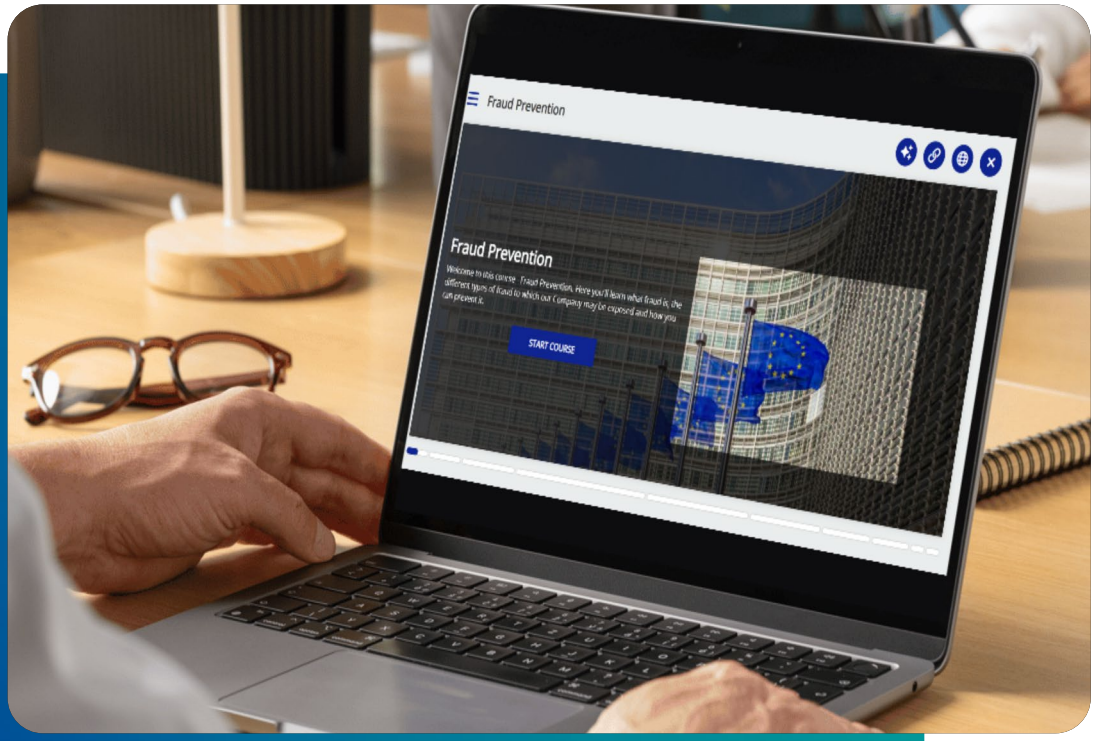
However, under the EU Payment Services Regulation (PSR) and PSD3, which is expected to become law in 2026, the burden of proof will shift from the victim to the institution. This means that firms, rather than the individuals they employ or serve, will carry the primary financial and legal risk for sophisticated fraud.

Here is what the new rules cover:

- **Greater liability:** If a fraudster initiates or changes a transaction, the Payment Service Provider (PSP) will be liable for that amount. Online platforms will also be liable to PSPs who have reimbursed customers if they are told about fraudulent content on their platform but fail to remove it. In spoofing cases – where a fraudster impersonates a bank employee to trick a customer – banks are now expected to reimburse the victim unless they can prove the user acted with gross negligence (a high legal bar to clear).
- **Mandatory name matching:** PSPs will have to check that a payee's name and unique identifier match for all credit transfers. Firms will be responsible for covering losses resulting from fraud if that verification mechanism fails.
- **Focus on human support**: Users must have access to human support (not just chatbots) to report fraud. Failure to provide a quick, human-led response can now be cited as a failure in the bank's duty of care.
- **Stronger transaction limits:** Payment service providers must enable customers to set their own spending limits and block payments where they suspect fraud.

To comply with the new PSD3 regulations, firms across Europe must go beyond identifying generic red flags and establish a culture of continuous learning. Training must be both regulator and real-life ready, with staff at every level given hands-on experience of the tactics modern fraudsters use.

Fraud is a global issue that ignores borders, so multinational organisations require standardised training to maintain consistency across jurisdictions. By using a centralised system like the Skillcast EU Compliance Library, firms can deliver high-quality, localised content that ensures every employee is trained to the same standard.



skillcast

Skillcast at ECEI Berlin, 2026

The 14th annual **European Compliance and Ethics Institute** (ECEI) conference takes place in Berlin from the 2nd to the 4th of March, and brings together compliance professionals from Europe and around the world to discuss the challenges of the year ahead.

Skillcast will be leading an educational session entitled “Inside the Fraudster’s Mind: What Compliance Leaders Need to Know in 2026.” We will be joined by Alex Wood, a convicted former fraudster who now advises government departments, including the UK Home Office, NHS, FCA, and FCDO on fraud prevention.

Having worked inside criminal organisations for decades, Alex is an expert on the psychology of fraud and provides a truly unique insight into how financial crime is evolving. He co-hosts the Radio 4 show Scam Secrets, and regularly speaks about fraud prevention across the public and private sectors.

To hear Alex’s talk, delegates can attend the Skillcast session at the ECEI conference on Monday, 2nd March at 10.20am.

Learn more