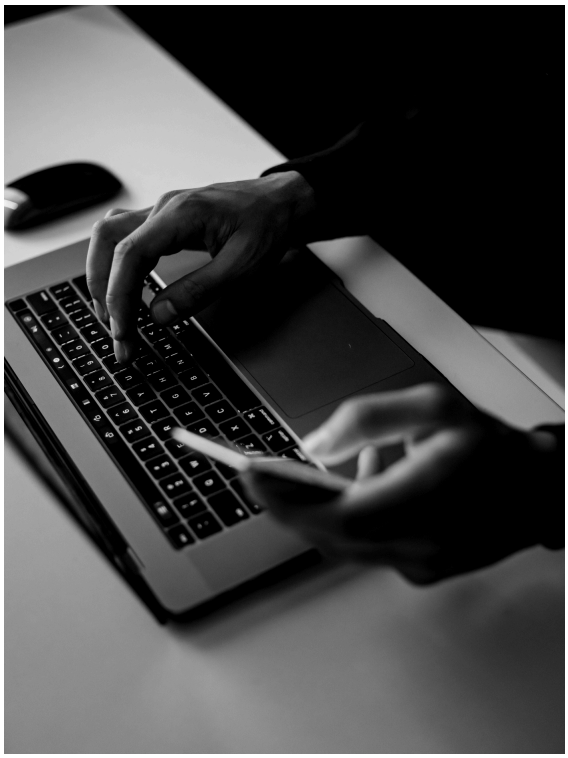
AMBAR

# Payment fraud: *is your company actually protected?*

DIGITAL FRAUD, PAYMENTS & DISPUTES

Payment fraud is no longer simply a cybersecurity issue. For companies it is increasingly a question of legal liability: when money is transferred to a fraudulent account, who ultimately bears the loss?



Business email compromise, CEO fraud and bank impersonation are becoming increasingly sophisticated. Many companies discover only after an incident that their contracts, payment procedures and insurance arrangements do not provide the protection they expected.

**When fraud occurs, the question is not who failed, but who bears the loss and what each party can prove.**

**488,426**
CYBERCRIMES RECORDED IN SPAIN IN 2025

**19.8%**
OF ALL RECORDED CRIME NATIONALLY

**88%**
WERE COMPUTER FRAUD

Spanish Ministry of the Interior data for 2025. Recorded cybercrime has grown 513.4% over the last decade.

The pages that follow set out how the fraud arrives, the five legal points worth reviewing, what to put in place before an incident, and what to do in the first 48 hours after one.

PART ONE · HOW IT ARRIVES

# The three patterns *affecting companies*

| | | |
|---|---|---|
| 01 | **Man-in-the-middle: the altered IBAN** | The fraudster intercepts correspondence between the company and its supplier and alters the IBAN shown on the invoice. The payment order is issued by the company itself, deceived — which is precisely what makes it hard to unwind. |
| 02 | **CEO fraud** | Impersonation of a director or of a supplier in order to instruct urgent and confidential transfers, typically during periods of weaker internal control: holidays, closing dates, a change of treasurer. |
| 03 | **Bank impersonation** | Smishing, vishing and unlawful duplication of the SIM card, used to intercept one-time codes and defeat strong customer authentication. |

## What the three have in common

In all three the money leaves through the company's own systems, with the company's own credentials, and often with its own authorisation. That is what moves the discussion out of cybersecurity and into contract, payment-services law and insurance — and it is why the documents signed long before the incident decide the outcome.

*The key question is no longer simply whether your systems can prevent fraud. It is whether your company is legally prepared when prevention fails.*

# Five points companies *should review*

| | | |
|---|---|---|
| 01 | **A fraudulent payment may still be an authorised payment** | In man-in-the-middle fraud the company itself authorises the transfer, having been deceived — a very different legal scenario from an unauthorised payment. Because the order is authorised, the rules on unauthorised transactions do not apply; instead, under Article 59 of the Payment Services Act, an order executed in accordance with the IBAN provided is deemed correctly executed. The Supreme Court has recently confirmed that criterion (Judgment 1733/2025 of 27 November), without prejudice to the provider's duties of recovery and cooperation under Article 59.2. |
| 02 | **Businesses may have less protection than consumers** | Article 34.1 of the Payment Services Act allows the parties, where the user is neither a consumer nor a microenterprise, to disapply, in whole or in part, among others, the rule requiring the provider to prove authentication and correct execution (Article 44) and the limits on the payer's liability for unauthorised transactions (Article 46); and, with any non-consumer user, including microenterprises, to agree a period other than thirteen months for notifying the transaction (Article 43). Such clauses appear routinely in framework agreements. The point is to establish what was actually signed with each bank, what room there is to renegotiate it, and how the company is classified, since that determines which protections cannot be waived. |
| 03 | **Verification of Payee changes the analysis** | Since 9 October 2025 in the euro area, Article 5c of Regulation (EU) 260/2012, as amended by Regulation (EU) 2024/886, obliges the payer's provider to offer a verification-of-payee service before authorisation, for credit transfers generally. Its paragraph 8 limits the provider's exemption for an incorrect identifier to cases where it complied; paragraph 6 lets non-consumer users opt out for batch orders — something a company may have done without weighing the consequences for the right to a refund. |
| 04 | **The dispute may not only be with the bank** | When an invoice is paid into an impersonated IBAN, a second controversy remains open with the supplier as to who bears the loss, under Articles 1162 to 1164 of the Civil Code. Has the company discharged its payment obligation, or can the supplier still demand payment? Two distinct fronts. |
| 05 | **The best defence starts before the fraud occurs** | Bank agreements, supplier-payment clauses, insurance cover and internal payment controls belong to the body of documents reviewed and approved before the incident, not after it. |

**REFERENCES** Arts. 34.1, 43, 44, 46 and 59 Royal Decree-Law 19/2018 (Payment Services Act) · Art. 5c Regulation (EU) 260/2012, as amended by Regulation (EU) 2024/886 · Arts. 1162 to 1164 Civil Code · Supreme Court Judgment 1733/2025, 27 November

PART THREE · BEFORE FRAUD HAPPENS

# What should companies *review?*

| | |
|---|---|
| **BANKING ARRANGEMENTS** | **Framework payment-services agreements.** Read the framework agreement and the general conditions signed with each bank, identifying the exoneration clauses agreed under Article 34.1 and the margin available to renegotiate them.<br><br>**Classification and verification arrangements.** Establish how the company is classified for the purposes of the Payment Services Act, which protections are therefore unwaivable, and how verification of payee is configured — including whether the company has opted out of it for batch payments. |
| **INTERNAL PAYMENT CONTROLS** | **A map of the payment circuit.** Who initiates payments, who validates them, against which thresholds, and with what segregation of duties in treasury.<br><br>**Supplier IBAN changes.** A protocol for adding and changing supplier bank details, with verification through an independent channel and a record of it — supported by dual validation above set amounts and a signature matrix. |
| **SUPPLIER CONTRACTS** | **Clauses on bank-account details.** Review the clauses governing account details and changes of bank account in contracts with suppliers, and introduce a standard notification clause into contracts and purchase orders. |
| **INSURANCE** | **Cyber-risk and liability cover.** Review the cyber-risk or civil liability policy specifically as regards social-engineering fraud, and identify the exclusions and the conditions on which cover depends. |
| **EVIDENCE & INCIDENT READINESS** | **Preservation of electronic evidence.** Criteria for preserving electronic evidence, with particular attention to the chain of custody.<br><br>**A first-48-hours protocol.** Approved in advance, with ready-to-use templates: communication to the bank, request for blocking and recovery of funds, complaint, notice to the insurer and, where applicable, notification to the data protection authority. |

PART FOUR · WHEN FRAUD HAPPENS

# The first *48 hours*

1 **Contact the bank or payment service provider** and request the blocking and recovery of the funds, in wording drafted so as not to prejudice the later claim.

2 **Preserve the electronic evidence,** with attention to the chain of custody.

3 **File the complaint,** with the technical detail needed to allow the funds to be traced.

4 **Notify the insurer** within the applicable time limit (seven days as a general rule under Article 16 of the Insurance Contract Act, unless the policy provides a longer period).

5 **Assess whether a personal-data breach notification is required** and make it where it is — within 72 hours of becoming aware of the breach (Article 33 GDPR).

6 **Decide the civil and criminal strategy,** and how the two are to be coordinated.

7 **Assess the position with the supplier or customer involved,** since the loss will also be discussed with them.

Criminal proceedings do not, as a general rule, prevent a civil ruling on authorisation, gross negligence, deficiency of the service and reimbursement.



THE EXPERT BEHIND THE INSIGHT

## Vanesa Fernández Escudero

AMBAR PARTNER · LITIGATION, CONSUMER LAW & DIGITAL FRAUD

Vanesa is a practising lawyer with more than 25 years of experience in litigation and arbitration, consumer law and compliance, with particular expertise in banking fraud and disputes arising from digital payment fraud. She is a lecturer at the Barcelona Bar Association, a member of the Advisory Board of the Consumer Law Section of the Madrid Bar Association, and an arbitrator at the Consumer Arbitration Board of Catalonia.

## Need to assess your company's exposure *to payment fraud?*

Book a call with Vanesa through Ambar.

BOOK A CALL →