Payment fraud: could one convincing email, call or video call move your money?

This quarter, write down how bank details may change (a call back to a number you already have, a second approver and a waiting period before the first payment) and have your bank require two signatures for payments. Then run Verification of Payee on your payment files too, and treat any request to skip the process as fraud, however senior the voice or face.

Reviewed	Next review	Version	Written for
5 Nov 2026	**5 Dec 2026**	**1.0**	**Finance, accounts payable, payroll and treasury teams, with the IT and security staff who support them**

Latest version
sheets.einblick.dev/payment-fraud/

If you only do five things

1. **Write down how bank details change, and let the system enforce it.**
   Accept new or changed bank details for suppliers and staff only after a call back to a number you held before the request and approval by a second person, then wait two business days before the first payment. In Dynamics 365 Finance, turn on the vendor bank account change proposal workflow and don't let imports use **Allow changes without approval**, which skips it[9].
2. **Require two people for large payments, at the bank too.**
   Above an amount you set, a second person approves in the ERP and a second signature releases at the bank; the German banking industry recommends joint signing for EBICS[7]. Give ERP and payment servers only a transport signature (T), which uploads files but can't authorize them[8].
3. **Run Verification of Payee on payment files.**
   Companies may skip the name check for files with several payments[1]. In German EBICS, the existing order types CCT and CIP skip it, while CTV and CIV run it[6]. Move supplier and payroll runs to the checking types, at least for payees whose details changed.
4. **Verify unusual requests outside the channel they came in.**
   Fake executives start on email or WhatsApp and follow up on video calls built from public footage[15,16]. Call back on a known number, agree code words for critical transactions[17] and agree that nobody is blamed for making the board wait while they check[7].
5. **Prepare the first hour.**
   Keep the bank's fraud line and who may call it on paper. The FBI's recovery team froze 58% of the $1.16 billion it tried to stop in 2025 and says time is of the essence[10].

The first hour after a fraudulent transfer

1. **Call your bank's fraud line.**
   Use the number from your contract or the bank's website. Ask for a recall with the reason fraud, which the bank can send once per payment[3], and for a freeze at the receiving bank. Transfers, instant or not, generally can't be revoked, and getting money back depends on the recipient's consent[5], so every minute counts.
2. **Stop the follow-ups.**
   In a Singapore case the fraudsters came back for another US$1.4 million; the bank's quick alert let police hold the US$494,000 already moved to Hong Kong[16]. Block the receiving IBAN, hold open payment runs, block EBICS users whose keys may be exposed and tell the bank[7].
3. **Report it to the police.**
   In Germany, use the state police cybercrime contact point (ZAC) listed in the incident response sheet. For transfers to US banks, also file at ic3.gov with the full transaction details, whatever the amount[10].
4. **Keep the evidence.**
   Save the emails as files with headers, chat messages, call logs, invoices, VoP results and bank confirmations before anyone deletes or resets anything. If a real mailbox sent the request, follow the incident response sheet.
5. **Warn whoever is next.**
   Tell the supplier or employee whose details were faked, and your insurer: this is usually a fidelity insurance claim, not a cyber claim[17] (see the cyber insurance sheet).

How companies lose the money

- **CEO fraud, now with deepfakes.** A Hong Kong employee paid about HK$200 million into five accounts after a group video call in which a pre-recorded deepfake of the UK head office's CFO gave instructions[15]. A voice can be cloned from a few minutes of recordings, often public ones[17], and Europol says AI makes BEC and CEO fraud more realistic[14].
- **Fake invoices and changed bank details.** Microsoft counted over 46 million attacks posing as executives, staff, suppliers or partners in a year, and one in four impersonation emails pushes the victim to a phone call[12].
- **Payroll diversion.** Attackers pose as employees and ask HR to change the salary account; 51% of the attempts Microsoft saw landed on a Monday or Tuesday[12]. Others take over the employee's own login: Storm-2657 changed salary bank details in Workday and hid the alert emails with inbox rules[13].

What Verification of Payee does and doesn't do

- **It checks name against IBAN.** The payee's bank reports a match, a close match with the registered name, no match or no check possible[2]. Euro area banks had to offer it free by 9 October 2025 (later joiners within a year), the rest of the EU by 9 July 2027[1].

Set up the bank side

- **Keep single signatures rare.** EBICS has single (E), first (A), second (B) and transport-only (T) signatures[8]; give E to as few people as possible.
- **Use chip cards, not key files.** Malware can copy key files with their passwords[7].

- **It never blocks.** You can pay after a warning, and a bank that ran the check correctly isn't liable[1].
- **Opted-out files lose it.** Non-consumers may opt out for payment packages[1]; BaFin tolerates it, for now, even for EBICS files with one payment[4].
- **A match is not proof.** It can't detect a fraudulent payee or request[5].
- **Register your trading names.** Ask your bank to store them as extra payee names, which BaFin allows[4], so customers see a match, not a warning.
- **Set limits that take time to raise.** A limit on all online transfers may have a waiting period for increases; one on instant transfers alone must be changeable at any time[4].
- **Review signing rights against HR.** Remove leavers and changed roles at the bank too[7].

Who owns what

- **Finance owns the process, not IT.** The CFO or head of accounting owns the bank detail rule, signing rights, limits, VoP settings and exceptions.
- **HR owns payroll changes.** Confirm each by phone, including self-service changes in the HR system.
- **IT protects the accounts.** Passkeys, starting with finance, HR and executives (passkeys and MFA sheet), DMARC and BEC detection (endpoints and email sheet), alerts on new inbox rules[13].
- **Management backs the no.** No exceptions requested by phone or chat.

What changed in 2026

- **BEC losses rose again.** Victims reported $3.05 billion to the FBI in 2025, up from $2.77 billion, including over $30 million in BEC involving AI[10].
- **Microsoft now tracks business contact impersonation.** It saw a 121% surge in April 2026; most first messages were bland small talk[12].
- **EU data shows who pays.** Tricked payers caused 74% of credit transfer fraud by value in 2024, up from 65%, and customers bore about 85% of credit transfer losses[11].

What you can skip

- **Spotting deepfakes, by tool or by ear.** The GDV calls the cues unreliable and says checking the request itself holds up better than judging picture or sound[17]. Teach the call back instead (security awareness sheet).
- **Call backs on every routine payment.** Spend them on new payees, changed details and unusual requests.
- **Paid name checks for euro payments.** Verification of Payee is free[1].

Mistakes that cost the most

- **Calling the number in the request.** Call one you already knew[17].
- **Paying through a no match.** After a warning the loss is usually yours[1,11]. Stop until the call back.
- **Letting secrecy beat the process.** The Singapore fraud used a fake lawyer, a confidential restructuring and a nondisclosure agreement[16].
- **Confirming changes to the same mailbox.** Attackers who control it delete the confirmation[13]. Use phone or letter.

What this looks like at your size

Small team, no security staff

- Write a one-page payment rule: call back on a known number, a second person for bank detail changes, no exceptions for the owner.
- Ask your bank how a second person can release online payments, and set a daily limit.
- Tell customers how you would announce new bank details.

Growing, with IT or security staff

- Enforce bank detail approval in the ERP and HR system, and close import paths that bypass it.
- Switch payment runs to the order types that run VoP, and route each no match to a second person.
- Alert on supplier and payroll bank changes and on new inbox rules in finance and HR mailboxes.

Enterprise or regulated

- Run treasury payments through EBICS with chip cards, A and B signatures and T-only server users.
- With the CEO's consent, have someone pose as them on video and check that finance calls back before paying.
- Report attempts and losses to the audit committee.

Version history

5 Nov 2026, version 1.0 Published after a copy edit and a source-by-source fact check, which tied Verification of Payee claims to the regulation's articles, corrected the trend in FBI loss figures and replaced dated deepfake detection data with the GDV's current advice.

Sources

1. Regulation (EU) 2024/886. EUR-Lex, 13 Mar 2024. eur-lex.europa.eu
2. VOP Rulebook v1.1. EPC, 16 Mar 2026. europeanpaymentscouncil.eu
3. SCT Rulebook 2025 v1.2. EPC, 30 Sep 2026. europeanpaymentscouncil.eu
4. FAQ Echtzeitüberweisungen. BaFin, checked 5 Nov 2026. bafin.de
5. FAQ Empfängerüberprüfung. Bundesbank, checked 5 Nov 2026. bundesbank.de
6. VOP im EBICS-Verfahren. Deutsche Kreditwirtschaft, 15 Apr 2025. ebics.de
7. EBICS-Sicherheitsempfehlungen. Deutsche Kreditwirtschaft, 4 May 2026. ebics.de
8. EBICS-Bedingungen, Anlage 1. Bundesbank, 5 Oct 2025. bundesbank.de
9. Vendor bank account workflow. Microsoft Learn, 20 Aug 2026. learn.microsoft.com
10. 2025 IC3 Annual Report. FBI IC3, Apr 2026. ic3.gov
11. 2025 Report on Payment Fraud. EBA and ECB, Dec 2025. ecb.europa.eu
12. Microsoft Digital Defense Report 2026. Microsoft, Oct 2026. cdn-dynmedia-1.microsoft.com
13. Payroll pirate attacks. Microsoft, 9 Oct 2025. microsoft.com
14. IOCTA 2026. Europol, 28 Apr 2026. europol.europa.eu
15. LCQ9 on deepfake fraud. HKSAR Government, 26 Jun 2024. info.gov.hk
16. Police recover over $670,000. Singapore Police, 7 Apr 2025. police.gov.sg
17. Voice-Cloning und KI-Avatare. GDV, updated 12 Aug 2026. gdv.de