CUSTOM SOFTWARE

A Supplier’s Bank Account Is the Riskiest Field in Your System

On 20 May 2026, the Singapore Police Force warned about a fraud that keeps recurring. Someone writes from an address that imitates a supplier’s, or from the supplier’s own compromised mailbox, and says the bank details have changed. The business pays the next invoice into the new account. At least 66 cases had been reported since 1 January, with losses of at least 19 million Singapore dollars.

The warning and its recommendations are in the Singapore Police Force advisory of 20 May 2026.
https://www.police.gov.sg/media-hub/news/2026/05/20260520_police_advisory_on_business_email_compromise_scams_involving_requests_to_update_vendors

In July, the US radio station WFAE interviewed a Wall Street Journal reporter about Surfside Beach, a South Carolina town that sent about USD 545,000 to an account in Utah instead of to its contractor. According to that account, someone posing as the contractor’s project manager asked for an electronic transfer instead of a cheque, and the fraudster had set up a domain almost identical to the contractor’s. Neither side noticed for 45 days, and the two sides disagree about where the failure happened.

The case is described in the interview published by WFAE on 27 July 2026.
https://www.wfae.org/business/2026-07-27/sc-beach-town-loses-500-000-in-phishing-scam

In January, Unit 42, the research team at the security company Palo Alto Networks, described a payroll case at an organisation it does not name. An attacker impersonated employees to several help desks, had passwords reset and multi-factor devices re-enrolled, and changed the salary deposit account for several people. It came to light when employees reported that their pay had not arrived.

A Change of Account Needs a Workflow of Its Own

In many systems, the bank account is just another field on the record. Whoever can correct an address can also change where the money goes, and the next payment run uses the new value without asking. A change should instead open a request with states (received, confirmed, approved, active), while payments keep going to the old account or stop.

- Never accept a change from the email or chat thread it arrived in: confirm it by calling a number that was already on the record.

- Require a second person to approve the change, and make sure it cannot be whoever entered it.
- Hold the first payment to a new account for an agreed period, or cap its amount until the supplier confirms receipt.
- Tell the previous contact about the change, using the email and phone number already on file.
- Alert the owner for every approved change and every first payment to a new account.
- Keep a visible log of who requested, confirmed and approved each change, with dates and masked details.

In Venezuela, suppliers are commonly paid by bank transfer, pago móvil or Zelle. For pago móvil the destination is a phone number, a cédula or RIF and a bank; for Zelle, an email address or a phone number. Those details, and each employee's payroll account, go through the same workflow. Picture a supplier messaging you on WhatsApp from a new number, asking for the next pago móvil to go to another phone. You log the request, call the number you already had, and the payment waits for someone else's approval. If the change is genuine, the supplier waits a day.

The First Hours Decide How Much Can Be Recovered

According to the annual report of the FBI's Internet Crime Complaint Center (IC3), published in April 2026, the centre received 24,768 business email compromise complaints in 2025, with reported losses of about USD 3.05 billion, second only to investment fraud. These are complaints filed with a US body and do not measure what happens in other countries. Its recovery team acted on 3,900 incidents across several kinds of fraud, not only this one, and froze about USD 679 million, which the FBI gives as a 58 per cent success rate. The report's advice is to contact your bank immediately and ask it to recall the funds, and to know in advance what help it offers, because each institution has its own policies.

The figures and the advice are in the FBI's IC3 2025 report, published in April 2026.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

- Call the bank the payment left from, on its official number, with the date, amount, reference and destination account to hand.
- Block payments to that payee in the system and check which other bank details changed in recent weeks.
- Contact the real supplier or employee through the details you already had, never through the request's thread.

- Keep the emails and messages complete, without deleting or editing them, and report the fraud to the authorities.

How We Build This in Custom Software

We start by mapping the process: who adds suppliers and employees, where account changes arrive from, who prepares the payment run and who approves it. Then we design the change of bank details as a workflow with separate roles for entering, confirming and approving, and the server checks those permissions even when the screen hides the button. The log records each step with an author and a time, and no role in the application can edit it. If payments are exported to a bank file, the integration reads approved details only. Automated tests try to approve one's own request, pay before the hold ends or change an account without permission, and confirm the system refuses. The handover includes documentation, training and a written guide to the first hours.

> *These controls make a payment to the wrong account less likely and shorten the response, but they do not eliminate fraud or replace protection of the email accounts. They work if the team uses them, and what can be recovered depends on the bank and the type of payment. This article is not legal advice.*

A Check You Can Run

Open the supplier and employee list in your payment system or spreadsheet and find every change to a bank account, pago móvil number or Zelle address in the last six months. For each one, note who asked for it, which channel it came through, who entered it and whether anyone confirmed it by calling a number already on file. If the system keeps no history, or one person can request, enter and pay, that is the first thing to fix. Then check in your online banking which users can register new payees. Only look: change nothing while you review.

Supporting guidance: The UK National Business Crime Centre's guidance on mandate fraud.
https://nbcc.police.uk/crime-prevention/cyber-and-fraud/bank-mandate-fraud

Continue with: Before Designing Screens, Decide Who Can Change What.
https://systems.kavaliero.com/en/blog/before-designing-screens-decide-who-can-change-what

For help with this work, see the scope of Custom Software.
https://systems.kavaliero.com/en/services/custom-software