

EXECUTIVE PAPER · INFRASTRUCTURE

Business Email Compromise Is a Payments Problem

Business email compromise cost American victims about $3 billion in 2025, and the money leaves through accounts payable. Chief financial officers should own the defense as a payments control, with email security behind it.

AUTHOR

Chris Watkins

SERVICE

Infrastructure

FOR

CFO, CEO, Controller · 12 min read

AT A GLANCE

The problem. Victims reported $3.05 billion in business email compromise losses to the FBI in 2025, the second-largest category of cyber-enabled fraud. The typical attack sends no malware. A criminal poses as a vendor or an executive and asks for a change of bank details or an urgent transfer, and an employee with authority to pay does what the message says.

Why it persists. Companies treat it as an email filtering problem and hand it to IT. Filters cannot stop a request sent from a vendor's real, compromised mailbox, a lookalike domain, a phone call, or a video meeting. The control that would stop it, an independent check before money moves, sits in finance and is often missing or skipped.

The recommendation. Make the CFO the owner. Verify every change to payment details by calling a number already in the vendor master, require an independent second approver above a set amount, hold the first payment to any changed account until the vendor confirms receipt, and treat any executive payment request by email, phone, or video as unverified until confirmed through a known channel. Keep email security as the second line.

The Decision in Front of You

Business email compromise, usually called BEC, is a fraud in which a criminal impersonates someone your company pays or obeys and redirects a payment to an account they control. The FBI defines it as a scam aimed at businesses that regularly pay suppliers by wire, carried out by compromising email accounts and other channels, including phone numbers and virtual meeting applications [1]. The decision is who owns the defense. Most companies give it to IT as a filtering problem. This paper argues that it belongs to the CFO as a payments control.

The losses are large and steady. The FBI's Internet Crime Complaint Center, known as IC3, received 24,768 BEC complaints in 2025 with reported losses of $3,046,598,558, second only to investment fraud among cyber-enabled crimes [1]. That is about $123,000 per complaint, and about 10% more in total than the $2.77 billion reported in 2024 [1][2]. Over 2023, 2024, and 2025 combined, reported BEC losses reached about $8.76 billion [1].

Finance teams see the attempts directly. In the Association for Financial Professionals' 2025 survey of 521 corporate treasury and finance practitioners, 63% reported attempted or actual BEC fraud in 2024, the most common avenue, and wires were the payment method most often targeted through BEC, cited by 63%, up from 39% a year earlier [3]. Coverage of the same survey reports that 36% of organizations lost money to BEC in 2024 [4].

What's Happening

The fraud is a change request, and the control point is finance

BEC attacks follow two patterns. In vendor impersonation, the criminal poses as a supplier and asks accounts payable to change the bank account or remittance address on file, then waits for the next scheduled invoice. In executive impersonation, the criminal poses as the CEO, CFO, or a deal lawyer and asks a staff member to send an urgent, confidential transfer. Both end with an authorized employee sending money through the company's own bank. No system has to be breached on your side.

The cases below come from a public company and city governments, which must disclose losses.

Six cases from 2024 and 2025

Orion S.A., 2024. The chemical company disclosed in an August 2024 filing with the Securities and Exchange Commission that an employee who was not a named executive officer had been the target of a criminal scheme that produced multiple fraudulent outbound wire transfers [5]. It expected a one-time pre-tax charge of about $60 million for funds not recovered, and said it had no evidence of unauthorized access to its systems or data [5]. The filing does not use the term BEC; coverage described it as the most likely explanation [5]. A single employee sent $60 million in several wires, and no payment control stopped them.

City of Baltimore, 2025. In December 2024, a fraudster used a personal email address to submit a fake contact for a real city vendor in the city's Workday system, and an accounts payable employee approved it without verifying the person [6]. In January the fraudster submitted fake voided checks and bank change requests, which two more employees approved in February [6]. The city paid $803,384.44 on February 21 and $721,236.60 on March 10, 2025, recovered the second payment, and lost the first [6]. The Inspector General found that city policy did not require phone verification of vendor contacts or bank changes, and that the same weaknesses had been flagged after frauds in 2020 and 2022 [6]. Two approvers signed off, and neither called the vendor.

City of Hamilton, Ontario, 2024. Between November 2023 and January 2024, a criminal who had compromised a vendor's email asked the city twice to change the vendor's bank details, and staff processed both [7]. The city lost C$274,000 and does not expect to recover it [7]. An internal audit found that staff had overlooked red flags despite fraud training a few months earlier, and had changed bank details on emailed requests alone [7]. In a separate case in March 2024, the city paid C$552,000 to a fraudster after changing bank details even though the real vendor had warned it not to [7]. A compromised vendor mailbox passes every email filter, because the messages really do come from the vendor.

Mercer Island, Washington, 2025. In January 2025, someone impersonating a city contractor by name and title asked the city to change the mailing address for payments [8]. Finance sent a check for $420,350.94 to the new address [8]. The city recovered $370,350.94, about 88%, through bank seizures

and its impersonation fraud insurance, leaving a net loss of the $50,000 deductible [8]. It then required secondary review and formal approval of vendor data changes [8].

Milwaukee, 2025. In late June 2025, scammers impersonating a library construction contractor emailed the city to change the vendor's bank account [9]. The message carried the company's signature and logo; the domain ended in ".us" in place of ".com" [9]. The city rerouted a $460,866 payment and learned of it weeks later from the real vendor; police traced the accounts and the bank froze and returned the funds [9].

An Oregon city government, 2025. The IC3 annual report describes an April 2025 BEC against a city government office in Oregon with a reported loss of more than $6 million [1]. The receiving account had already been frozen after an earlier complaint, so the receiving bank asked the originating bank to confirm the wire instructions, which were found to be fraudulent, and the $6 million wire was recalled [1]. The money came back because an earlier victim had reported the same account quickly.

SIDEBAR: VOICES AND FACES ARE NO LONGER PROOF

In 2024 an employee in Arup's Hong Kong office made 15 transfers totaling about US$25.6 million after a video call in which the CFO and colleagues were deepfakes [10]. FinCEN, the Treasury's financial crimes unit, warned in November 2024 that criminals have used generative AI to impersonate executives and instruct staff to transfer large sums [11]. The FBI said in December 2025 that AI-generated voice messages are being used to impersonate senior officials and that AI content is often difficult to identify [12]. IC3 counted more than $30 million in 2025 BEC losses that involved AI [1]. Any procedure that accepts a familiar voice or face as verification needs replacing.

Why the Usual Approach Fails

The usual response to BEC is to buy better email filtering and run phishing training. Both help, and neither controls the payment.

Filters look for malicious links, attachments, and spoofed senders, and a typical BEC message has none. It is a polite request for a bank change sent from a lookalike domain, as in Milwaukee [9], or from the vendor's real mailbox, as in Hamilton [7]. Increasingly the request arrives by phone or video, where no email filter applies [1][10].

Training decays under pressure. Hamilton's staff had fraud training months before they processed two fraudulent changes [7]. Attackers create urgency and impersonate people staff do not want to question.

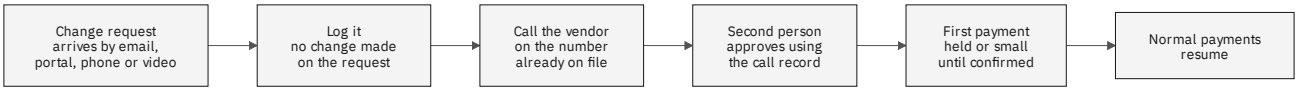
Dual approval often fails in practice. Baltimore had two employees approve the bank change, and both relied on the documents the fraudster supplied [6]. A second approver who looks at the same email adds no protection. The second check has to use a channel the attacker does not control.

Recovery is treated as an afterthought. The IC3 Recovery Asset Team froze $679 million of $1.16 billion in attempted theft across 3,900 incidents in 2025, a 58% success rate, and its domestic process froze 61% of reported losses [1][13]. Its guidance is to call your bank and request a recall as soon as fraud is recognized, then file with IC3 [1]. Freezes depend on speed. AFP respondents reported that only 22% of organizations recovered three-quarters or more of funds lost to payments fraud in 2024, down from 41% the year before [3].

The Framework: The Payment Change Control

The Payment Change Control is a short set of rules owned by the controller and enforced in the payment system. Exhibit 1 shows the path every change request takes.

Exhibit 1. A change to payment details takes effect only after a callback to a known number and a confirmed first payment



Source: author's framework, consistent with IC3 guidance to verify payment changes with the intended recipient [13].

Callback from the vendor master. Any request to change bank details, remittance address, or the vendor's contact person is verified by phone using a number already in the vendor master or in the signed contract. Never use a number, link, or contact given in the request itself. IC3's guidance to businesses is to make no payment change without verifying it with the intended recipient [13]. Record who called, the number, and who confirmed.

Independent second approval above a threshold. Changes to vendor banking data and any payment above a set amount need a second approver who did not handle the request and who reviews the callback record. The second approver checks the verification itself, which the fraudster cannot supply.

Hold the first payment. The first payment to a new or changed account is held for a set period, or sent as a small test amount, until the vendor confirms receipt through the known number. Baltimore, Hamilton, and Milwaukee all found out when the real vendor asked why it had not been paid [6][7][9]. A hold moves that discovery ahead of the loss.

Assume voices and video can be faked. No payment moves on instruction from an executive by email, text, phone, or video call alone. Staff confirm through a second channel they initiate, such as a call to the executive's known number or a message on an internal system. The FBI's 2025 guidance gives the same instruction: verify independently by calling a number you have confirmed yourself, and treat requests for money with skepticism [12]. Executives sign the rule, and staff who delay a payment to verify it face no penalty.

A first-hour recovery plan. Treasury keeps one page with the bank's fraud desk number: on discovery, request a recall, then file at ic3.gov with full transaction details [1][13].

Email security stays in place as the second line: multi-factor authentication on mailboxes, with phishing-resistant methods where possible, as FinCEN recommends [11], plus authentication of your own domain and monitoring for lookalike domains such as the one used against Milwaukee [9]. These cut the attempts that reach accounts payable; the payment controls decide whether one that gets through costs money.

Banks and payment networks are moving in the same direction. Nacha, which governs the ACH network, has said that rule changes taking effect in 2026 aim to reduce successful fraud such as BEC and improve recovery [14].

What it costs to run

Consider the author's illustrative estimate. A company with 2,000 active vendors sees 5% of them change bank details each year, or 100 changes. Each callback and second review takes 20 minutes, about 33 hours a year. At a loaded cost of $60 an hour that is about $2,000 a year in staff time. The average BEC complaint to IC3 in 2025 reported a loss of about $123,000 [1]. Under these assumptions, one prevented loss pays for the control for decades.

Costs, Risks, and Tradeoffs

Exhibit 2. Finance-owned controls cost staff time and some vendor friction

Area	Cost or risk	Mitigation
Staff time	Callbacks and second reviews on every banking change	Small volume in most companies; route changes to one trained team
Vendor friction	Vendors wait for the first payment and must answer calls	Explain the rule at onboarding and on the change form
Executive friction	Leaders find verification slow during deals or travel	Executives sign the rule; pre-agree a verification channel for travel
Stale vendor master	Callback numbers are wrong or were changed by the fraudster, as in Baltimore [6]	Treat changes to contact data as a banking change; verify them the same way
Over-reliance on email security	A filter cannot stop requests from a real vendor mailbox [7]	Keep filtering as the second line; measure the payment controls directly
When this is wrong	A business that pays almost entirely by card or through a payments platform that verifies payee bank accounts itself carries less of this exposure	Confirm what the platform verifies; keep the executive impersonation rule, which covers wires outside the platform

Source: author's analysis.

How to Act

Exhibit 3. A one-year roadmap

Window	Actions	Owner	Milestone
First 30 days	Freeze changes to vendor banking data made on emailed requests. Start callbacks from the vendor master. Publish the executive impersonation rule, signed by the CEO. Put the bank fraud desk number and IC3 steps on one page.	CFO with controller	100% of banking changes since the start date have a callback record; rule signed and sent to everyone who can release payments
First 90 days	Set dual-approval thresholds in the ERP and bank portal. Add a hold on first payments to changed accounts. Audit the vendor master for changes in the past 12 months and re-verify each one. Turn on phishing-resistant MFA for finance mailboxes.	Controller with CIO	Thresholds enforced in the ERP and bank portal; all past-year changes re-verified; finance mailboxes on phishing-resistant MFA
First 365 days	Run unannounced tests: a fake bank change request and a fake executive call. Rehearse the recovery plan with the bank. Report attempts, blocked changes, and test results to the audit committee.	CFO with internal audit	Two tests a year with every fake request stopped at callback; recall request placed within one hour in the rehearsal; quarterly report to the audit committee

Source: author's recommendation.

Questions to Ask Your Team

1. In the last year, how many vendors changed bank details, and how was each change verified?
2. Where does the callback number come from, and could a fraudster have changed it first?
3. Which person in our company could send $1 million today without a second approver?
4. What would our staff do if the CEO called on video and asked for an urgent, confidential wire?
5. How long would it take us to call our bank and request a recall after spotting a fraudulent payment?
6. Who owns this control: finance, IT, or no one?
7. When did we last test our payment controls with a fake request?

Closing

Business email compromise moves money through your payment process, using your own staff and your own bank. Better email filtering reduces the attempts that reach accounts payable, and only finance can stop the payment. Make the CFO the owner, verify every change to payment details through a number already on file, require an independent second approver above a threshold, hold first payments

to changed accounts, and treat any voice or video request for money as unverified until confirmed. These controls cost hours of staff time a year, against reported losses that average six figures per incident.

Sources

[1] Federal Bureau of Investigation, Internet Crime Complaint Center. "2025 IC3 Annual Report." 2026. https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf.

[2] Federal Bureau of Investigation, Internet Crime Complaint Center. "2024 IC3 Annual Report." 2025. https://ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[3] Association for Financial Professionals. "Survey: 79% of Organizations Were Victims of Attempted or Actual Payments Fraud Activity in 2024." 2025 AFP Payments Fraud and Control Survey. 2025. https://www.financialprofessionals.org/about/learn-more/press-releases/Details/survey-79-percent-of-organizations-were-victims-of-attempted-or-actual-payments-fraud-activity-in-2024.

[4] Digital Transactions. "Business Email Compromise Remains the No. 1 Fraud Attempt Avenue." Coverage of the 2025 AFP Payments Fraud and Control Survey. 2025. https://www.digitaltransactions.net/business-email-compromise-remains-the-no-1-fraud-attempt-avenue/.

[5] Help Net Security. "Scammers dupe chemical company into wiring $60 million." Coverage of Orion S.A. Form 8-K. 2024. https://www.helpnetsecurity.com/2024/08/13/orion-fraudulent-wire-transfers-60-million/.

[6] CBS News Baltimore. "Baltimore City Inspector General report on vendor payment fraud scheme." 2025. https://www.cbsnews.com/baltimore/news/baltimore-city-oig-fraud-scheme.

[7] The Public Record. "$274,000 stolen from the City of Hamilton in business email compromise fraud." 2025. https://thepublicrecord.ca/2025/05/274000-stolen-from-the-city-of-hamilton-in-business-email-compromise-fraud/.

[8] KOMO News. "Mercer Island recovers 88% of $420K city paid to fraudulent contractor in another state." 2026. https://komonews.com/newsletter-daily/mercer-island-recovers-88-of-420k-city-paid-to-fraudulent-contractor-in-another-state-fraud-construction-check-taxes-taxpayer-irk-banking-money-economy-investigation.

[9] FOX6 News Milwaukee. "Milwaukee recovers nearly $461K after fraud scheme targets city vendor." 2025. https://www.fox6now.com/news/milwaukee-recovers-nearly-461k-after-fraud-scheme-targets-city-vendor.

[10] Fortune. "A deepfake 'CFO' tricked the British design firm behind the Sydney Opera House in $25 million scam." 2024. https://fortune.com/europe/2024/05/17/arup-deepfake-fraud-scam-victim-hong-kong-25-million-cfo.

[11] Financial Crimes Enforcement Network. "FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions." FIN-2024-Alert004. 2024. https://www.fincen.gov/sites/default/files/shared/FinCEN-Alert-DeepFakes-Alert508FINAL.pdf.

[12] Federal Bureau of Investigation, Internet Crime Complaint Center. "Senior U.S. Officials Continue to be Impersonated in Malicious Messaging Campaign." Public Service Announcement I-121925-PSA. 2025. https://www.ic3.gov/PSA/2025/PSA251219.

[13] Federal Bureau of Investigation, Internet Crime Complaint Center. "Domestic Financial Fraud Kill Chain (D-FFKC) Process." https://www.ic3.gov/Outreach/Brochures/IC3-FFKC_Domestic.pdf.

[14] Nacha. "FBI's IC3 Finds Almost $8.5 Billion Lost to Business Email Compromise in Last Three Years." 2025. https://www.nacha.org/news/fbis-ic3-finds-almost-85-billion-lost-business-email-compromise-last-three-years.

The views in this paper are the author's own and do not represent any employer. Scenarios are hypothetical. This paper is not legal, financial, or compliance advice.