Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/business-email-compromise-first-24-hours/

ENTERPRISE INCIDENT RESPONSE

The First 24 Hours of a Business Email Compromise

A misdirected wire and a hijacked email thread leave two clocks running at once: the bank's recall window and the tenant's log retention. Freeze both records first and clean up the mailbox once they are captured, then call (800) 868-8189 at any hour.

Published September 5, 2026 · Updated October 30, 2026

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

The Critical Window for Wire Recall and the Audit Trail

The first twenty four hours following the discovery of a business email compromise or misdirected wire transfer shape both the wire recall effort and the technical record that liability turns on. The strongest responses export the mailbox configuration first, capturing the inbox forwarding rules, the session records and the credential history before IT administrators delete rules or reset passwords. That order keeps the exact timestamps, external forwarding addresses and session identifiers that retained legal counsel and cyber insurance adjusters use to determine whether the compromise occurred inside your tenant or within a vendor network.

Coordinating Financial Recall, Identity Containment and Forensic Analysis

An effective first day response runs three parallel tracks under the guidance of the legal team, internal audit and corporate security leadership. First, corporate treasury and finance teams must contact the originating and receiving financial institutions immediately to request a wire recall and freeze recipient accounts while documenting every payment instruction modification. Second, Global Digital Forensics works alongside your IT administrators to capture a forensically sound snapshot of Microsoft 365 or Google Workspace unified audit logs, transport rules, delegate permissions and hidden RSS or Archive folder rules before evicting the intruder from active sessions. Third, our examiners analyze cross tenant email transport headers and authentication signatures to establish where the thread hijacking originated.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The Bank, the Statute and the Recall Record

Finance teams move faster when they know how the law treats a fraudulent wire. Wire transfers between commercial accounts are governed in most states by Article 4A of the Uniform Commercial Code, which allocates loss according to whether the bank and the customer followed an agreed security procedure and whether the payment order was authorized or verified in good faith under that procedure (UCC Article 4A). The practical consequence is that the record of how the payment instruction was received, who approved it and what verification was performed will be examined by the bank, the insurer and possibly a court. We preserve that record alongside the mailbox evidence so the two accounts can be reconciled.

The FBI's Internet Crime Complaint Center at ic3.gov accepts business email compromise complaints and is the channel through which the Bureau coordinates with financial institutions on recall attempts. Filing promptly with accurate transaction details, the originating and beneficiary bank information and the dates of the fraudulent instructions gives the recall effort its best footing. We help the finance and legal teams assemble the technical facts the complaint asks for, including the sending domain, the message identifiers and the timestamps of the fraudulent instructions in UTC, and we keep copies of what was filed so the account given to the insurer matches the account given to the government.

The recall track and the forensic track protect each other. The bank wants to know whether the customer's own systems were compromised, because that bears on loss allocation. The insurer wants to know the same thing for coverage. The forensic record answers it from the tenant logs and message headers, and a finance team that preserves its payment approval emails, its vendor master change records and its call logs lets us tie the technical timeline to the business decision. That is why the first call to us often happens while the treasury team is still on the phone with the bank, and why we ask finance to keep every record where it is.

What Headers and Audit Logs Establish, and How They Combine

A fraudulent payment instruction carries its own evidence in the message headers. The Received chain shows the servers the message passed through and when. The Authentication Results header shows whether SPF, DKIM and DMARC passed for the claimed sending domain, and a lookalike domain registered days before the fraud shows up plainly when the headers are read from the original .eml or .msg file rather than a forwarded copy. Our zero upload Email Header Analyzer (evestigate.com/tools/email-header-analyzer/) lets anyone on the response team look at those fields immediately. Who controlled the sending account, and whether the counterparty's mailbox was the one compromised, is examined by combining the headers with sign in records and the counterparty's own logs, and the report sets out which source carries each point.

The tenant audit record extends the picture inside your own environment. Inbox rule creation events show whether the intruder set rules to move replies from the real vendor into RSS Feeds or Archive folders, which is the classic method for keeping a hijacked thread alive. Sign in records show whether the rules were created by a foreign session, and MailItemsAccessed records show which folders were synchronized. Together these records are where we look for whether your tenant was accessed, when, and what the intruder did to steer the conversation. Whether the vendor was also compromised is examined in the vendor's own logs, which counsel arranges through a cooperative agreement.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Reading these records well means separating three propositions: that a fraudulent message arrived, that your tenant was accessed, and that the two are connected. In many matters the first is true, the second is false and the compromise lived entirely at the counterparty, which changes the liability analysis considerably. We structure the report around those three propositions so each is supported by its own evidence and a reader can see which one the records actually reach. Our business email compromise analysis page describes the sources this draws on. A reader who takes the report in that order matches each assertion to the record that supports it.

How the Examination Runs in the First Days

The first hours are preservation. Under the direction of counsel we export the Unified Audit Log results for the affected mailboxes, the Entra or Google sign in records, the full inbox rule and transport rule inventory, delegate and forwarding settings, and the original fraudulent messages with their headers, and we hash and log every export. We ask administrators to complete the exports first and clean up afterward, because the export captures each rule's own conditions and target folder, while a deleted rule leaves only its deletion event. Where retention is short, this step takes precedence over everything except active loss prevention.

Analysis then runs on two fronts. The header and authentication review establishes the external path of the fraudulent instructions and the registration history of any lookalike domain. The tenant review reconstructs the intruder's session timeline, rule changes and folder access, and identifies the entry point, whether an adversary in the middle phishing page, a compromised personal device or a third party application. We correlate the two so you can see whether the thread was hijacked inside your tenant, at the vendor, or both, and when the attacker first had visibility into the payment conversation.

The last phase addresses exposure and recurrence. If the session synchronized folders containing personal data, health information or client confidences, counsel needs an inventory for the notification analysis described below. The security team needs to know which controls to strengthen and which would have caught it. We deliver the factual timeline, the exposure inventory and the control observations as separate sections of one report, so each audience can act on its part and the document can be converted into a declaration for the insurer or a court without rewriting. The incident response retainer page describes how organizations arrange this coverage in advance.

Notification Duties That Depend on What the Record Shows

Whether anyone must be notified turns on facts the examination establishes: what data the intruder could reach, whether it was actually acquired or accessed, and which laws apply to it. For protected health information, the HIPAA breach notification rule requires notice to affected individuals “without unreasonable delay and in no case later than 60 calendar days after discovery of a breach” (45 CFR 164.404), and the HHS breach notification guidance describes the risk assessment that precedes that decision. Counsel makes the determination. Our role is to supply an accurate picture of which folders and files were within the session's reach and which the logs show were actually synchronized.

New York's SHIELD Act, codified at General Business Law 899-aa, requires notice to affected New York residents within 30 days of discovery, and to the Attorney General, the Department of State and the State Police, when private information is accessed or acquired, and the Attorney General's reporting page explains

© 2026 Global Digital Forensics, Inc. All rights reserved.

the filing. Financial services companies regulated by the Department of Financial Services carry separate obligations under 23 NYCRR Part 500. Our guide to SHIELD Act incident facts explains how the examination record feeds those filings, and the same factual inventory serves the notification statutes of other states. The same inventory serves the notice requirements in the cyber insurance policy.

Public companies have an added layer. The Securities and Exchange Commission adopted rules in 2023 requiring disclosure of material cybersecurity incidents within four business days of determining materiality, as described in the Commission's announcement. A business email compromise that moves a large payment or exposes deal information can trigger that analysis, and the determination depends on facts the forensic timeline supplies: what was accessed, for how long, and whether the intrusion is contained. We write the timeline so disclosure counsel can quote it without reconstructing it. Disclosure decisions made on an accurate forensic timeline stand on the facts.

What to Prepare Before Engaging a Cloud Forensic Examiner

Assemble the affected user email addresses, the approximate date range of the disputed financial communications, original .eml or .msg copies of the fraudulent payment instructions and Global Administrator contact details first, then make manual changes to a compromised mailbox. Keep disputed emails in the mailbox as received, with the cryptographic DKIM signatures and routing headers that attribution relies on.

Test your raw message headers safely in your browser with our Email Header Analyzer (evestigate.com/tools/email-header-analyzer/) and call Global Digital Forensics immediately at (800) 868-8189 so our senior examiners can support your legal and security teams while the rolling cloud logs are within retention. The initial consultation is free.

Four Tracks Across the First Day

The guide describes a first day response that runs on parallel tracks rather than in sequence. This table sets those tracks side by side so each owner can see what belongs to the first hour, what follows once the recall request is in, and what must be in hand by the end of the day. The rows are roles rather than people, because in a smaller organization one person may hold two of them. The finance and legal rows move at their own pace alongside the forensic work, which is the point of running them together.

Responsibilities by role during the first twenty four hours after a misdirected wire is discovered.

Track	First hour	Hours one to four	By end of day one
Finance and treasury	Call the sending bank fraud desk with reference, beneficiary and amount	File with IC3 using UTC timestamps and message identifiers	Preserve approval emails, vendor master changes and call logs
Identity and IT	Run the exports first, then delete rules and reset passwords	Export audit log, sign in records, rules, delegates and forwarding	Hash each export and record who ran it from which admin account
Forensic examiner	Collect the fraudulent messages as original .eml or .msg files	Read headers and authentication results for the sending path	Reconstruct foreign sessions and folder access in the tenant

© 2026 Global Digital Forensics, Inc. All rights reserved.

Track	First hour	Hours one to four	By end of day one
Legal	Direct the response and decide who speaks to the counterparty	Send preservation requests to the vendor and to internal IT	Decide on insurer notice and which propositions the record reaches
Vendor liaison	Ask the vendor to hold its own logs and original messages	Learn whether the vendor tenant also shows unfamiliar sessions	Arrange a cooperative exchange of records through counsel

Read the Wire Email Headers in the Email Header Analyzer

Take the email that carried the changed wire instructions, export it as an .eml or .msg file from the mailbox that received it, open it and copy the full header block into the Email Header Analyzer (evestigate.com/tools/email-header-analyzer/). Read the Received hops from the bottom up, which is the order the message actually traveled, and compare the originating server with the hops on a genuine message from the same vendor. Then read the authentication results. A DKIM signature that verifies for a lookalike domain is a different problem from a failed signature on your real vendor domain, and the analyzer separates the two. Keep the exported file untouched for the examiner. When the hops point inside your own tenant or the vendor has no account of the message, call first and change rules after the exports.

How to Begin and What Happens on the First Call

Our Business Email Compromise Checklist: Preserve Before You Clean Up sets out the items to secure in the order they expire. For the first call, have the fraudulent messages saved as original files, the payment and approval records, the names of the finance, identity and legal owners, a Global Administrator contact and a note of any containment already done. The examiner asks when the fraud was discovered, whether the wire has been recalled, whether the vendor has been contacted, what has changed in the tenant, and whether counsel is directing the response. The same conversation produces a written proposal: the sources to preserve, the order in which to preserve them, the questions the analysis will answer and the form of the deliverable, with timing tied to your tenant's retention and licensing. The initial consultation is free. Call (800) 868-8189 at any hour.

Technical References and Further Reading

Primary sources and provider documentation behind this guide: FBI business email compromise guidance and Microsoft's compromised account response guidance.

Authorities cited in this guide: Uniform Commercial Code Article 4A, Funds Transfers. Establishes the security procedure framework that governs loss allocation for commercial wire transfers, text as published by Cornell LII. 45 CFR 164.404, Notification to individuals. Supplies the HIPAA notification deadline quoted in the guide, current text at Cornell LII. New York General Business Law 899-aa. Establishes the SHIELD Act notification duty for private information of New York residents, current text at the New York State Senate site. SEC press release 2023-139 on cybersecurity disclosure rules. Establishes the four business day disclosure requirement for material cybersecurity incidents adopted by the Commission in July 2023.

© 2026 Global Digital Forensics, Inc. All rights reserved.

FREQUENTLY ASKED

Wire Recall, Notice and Vendor Logs

Can a fraudulent wire transfer be recovered?

Recovery is possible, and speed matters most. Recovery depends on how fast the originating bank requests a recall, whether the beneficiary bank still holds the funds, and whether the FBI's Internet Crime Complaint Center can coordinate a freeze. Treasury contacts both banks and files at ic3.gov immediately, alongside the forensic work. Our part is to supply accurate dates, message identifiers and sending domains for those filings and to preserve the records the bank and insurer will later ask about.

How do we know whether our mailbox or the vendor's was compromised?

Your own tenant logs answer half the question. If sign in records show a foreign session, inbox rules were created to hide replies, or folders were synchronized by an unfamiliar client, your tenant was accessed. If those records are clean and the fraudulent messages came from a lookalike domain that passed its own authentication, the compromise may have lived at the counterparty. The vendor's logs, which your attorneys can request under a cooperative agreement between the parties, are where that question is examined.

What do you need from us on the first day?

The affected mailbox addresses, the original fraudulent messages as .eml or .msg files rather than forwards, the approximate date range of the payment conversation, a Global Administrator contact, the tenant license tier and a list of any changes already made to rules, passwords or sessions. We also want the payment approval trail from finance so the technical timeline can be tied to the business decision. We arrange a secure transfer on the call.

How do insurers use the forensic report?

Cyber and crime policies often turn on whether the insured's own systems were compromised, whether a security procedure was followed on the payment, and how quickly the loss was discovered and reported. The report answers the first two from the tenant logs and headers and documents the third from the timeline. We write the factual findings separately from control observations so the insurer gets the facts it needs and the legal team evaluates the control questions on its own schedule.

Do we have to notify anyone after a business email compromise?

That is a legal determination, and it depends on what the intruder could reach and what the logs show was synchronized or acquired. Health information, New York resident data, regulated financial services data and public company materiality each carry their own rules and deadlines. The examination supplies the inventory of folders and files within the session's reach and the dates of access, the facts those rules are applied to.

Web Addresses for the Sources Cited

1. UCC Article 4A: https://www.law.cornell.edu/ucc/4A
2. ic3.gov: https://www.ic3.gov/
3. 45 CFR 164.404: https://www.law.cornell.edu/cfr/text/45/164.404

© 2026 Global Digital Forensics, Inc. All rights reserved.

4. HHS breach notification guidance: https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html
5. General Business Law 899-aa: https://www.nysenate.gov/legislation/laws/GBS/899-AA
6. Attorney General's reporting page: https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act
7. 23 NYCRR Part 500: https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500
8. Commission's announcement: https://www.sec.gov/newsroom/press-releases/2023-139
9. FBI business email compromise guidance: https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise
10. Microsoft's compromised account response guidance: https://learn.microsoft.com/en-us/defender-office-365/responding-to-a-compromised-email-account

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed November 3, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.