Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/fbi-cyber-scam-warning-bec-scams/

WIRE FRAUD ATTRIBUTION

Forensic Attribution in Vendor and Real Estate Wire Fraud

A diverted wire puts two companies at odds while the money moves through mule accounts, and the examiner reads the record on each side for the failure. Ask your bank for a recall, report to IC3, and have counsel retain an examiner, who preserves the mailboxes first. Call (800) 868-8189 at any hour.

Published February 2, 2015 · Updated October 30, 2026

Primary Reference for This Guide

Start with FBI guidance on business email compromise.

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

How Loss Is Allocated When a Wire Transfer Is Diverted

When a corporate treasury department, real estate title company or private equity fund wires hundreds of thousands or millions of dollars to a fraudulent bank account after receiving updated ACH or wire instructions via email, an urgent legal dispute immediately erupts between the sender and the intended recipient. Under Uniform Commercial Code principles and commercial contract law, courts frequently allocate liability based on comparative fault, asking which party email system was actually compromised and which party failed to exercise ordinary care to detect spoofed domains, altered reply to headers or unauthorized mailbox rules.

Attribution Across Both Parties' Email Environments

Global Digital Forensics conducts business email compromise and wire fraud attribution engagements directly for retained litigation counsel, corporate general counsel and fidelity insurers. Rather than relying on surface printouts of the fraudulent email thread, our examiners inspect the raw .eml and .msg containers, cryptographic DKIM signatures, SPF alignment records and SMTP hop latencies alongside the Microsoft 365 or Google Workspace unified audit logs of the relevant tenants. We examine whether an intruder hijacked an authentic mailbox inside one party or the other using stolen session tokens, or whether an external actor registered a lookalike cousin domain to deceive an unverified payment workflow.

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

First Hours: Recall, Reporting and Who Speaks for the Company

The sequence in the first hours matters more than anything the examiner does later. The treasurer or controller who released the payment calls the sending bank's fraud desk, asks for a recall of the wire and gives the reference number, the beneficiary account and the amount. The sending bank contacts the beneficiary bank, and if the funds are still sitting in the receiving account they can sometimes be frozen. At the same time someone files a complaint with the FBI Internet Crime Complaint Center, whose Recovery Asset Team works with financial institutions on freezing fraudulent transfers. That is the recovery work, and it runs in parallel with evidence preservation.

Counsel should direct the legal position from the first call. Outside or general counsel decides who notifies the counterparty, what is said to the bank in writing, whether the insurer receives notice and when, and how the examiner is engaged so the analysis runs under the direction of counsel. We ask counsel to send two short holds the same day: one to internal IT freezing any change to the affected mailboxes, rules, sign in logs and audit configuration, and one to the counterparty requesting that it preserve its own tenant logs and the original messages. Those letters cost little and keep both sides honest when the comparative fault question is argued months later. Our guide to the first 24 hours of a business email compromise lays out the division of labor between legal, finance and security in more detail.

What UCC Article 4A Asks About a Payment Order

Two different disputes hide inside a diverted wire. The first is between the sending company and its own bank, and UCC Article 4A governs it. Article 4A defines a security procedure as one established by agreement for the purpose of "verifying that a payment order or communication amending or cancelling a payment order is that of the customer," and Section 202 makes a payment order effective against the customer, whether or not authorized, when the bank accepted it in good faith under a security procedure that is "a commercially reasonable method of providing security against unauthorized payment orders." If the customer's own authorized user typed the payment order after being deceived by a fraudulent email, the bank usually did exactly what the procedure required, and the loss generally stays with the customer.

The second dispute is between the sender and the intended payee, and it is a contract and negligence question decided outside Article 4A. Courts asked which party's mailbox was compromised and which party failed to notice obvious warning signs look for facts: whether the fraudulent instructions originated from inside the vendor's real tenant, whether the sender's own accounts payable mailbox had a forwarding rule planted weeks earlier, whether a lookalike domain was registered days before the request, and whether anyone verified the change by calling a known number. Our job is to put those facts on the table with the records behind them so counsel can argue the allocation. The report sets out the technical facts, and counsel argues the law.

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

What the Email Record Can Settle

Message headers show the route a message took and which servers handled it, and DKIM and SPF results show whether the sending domain authorized that path. The Microsoft 365 unified audit log and the Google Workspace log events show when a mailbox was accessed, from what IP address and client, and when an inbox rule or forwarding address was created. Entra sign in logs show whether a session passed or bypassed multi factor authentication. Taken together, those records can establish that a specific mailbox was under someone else's control during the window in which the payment instructions were sent, which is usually the fact the dispute turns on. You can inspect the raw headers of a suspect message yourself with our Email Header Analyzer (evestigate.com/tools/email-header-analyzer/) before anything is collected.

Counsel benefits from knowing how each record is read before the complaint is drafted. A sign in from an unfamiliar country shows a session, and tying it to a person combines it with device, network and provider records. An inbox rule named with a single period shows intent to hide messages, and the audit log entry for its creation records the session that created it, which the examiner traces. A header that passes DKIM shows the sending tenant signed the message, and the mailbox audit trail is where authorship is examined. Retention windows set the period each source covers: Microsoft documents a default audit retention of 180 days for standard licensing on its audit log retention page, and Entra sign in logs are retained for a far shorter period under many licenses. For a compromise that started earlier, the examiner reconstructs the earlier period from message artifacts, mail flow traces and the counterparty's records, and the report states plainly which source covers each period.

From Tenant Logs to a Declaration Ready for Filing

The engagement runs in phases, and each phase exists to protect the client. Scoping identifies the mailboxes, tenants and date range in play and the questions counsel needs answered, so the collection is proportional and the cost is predictable. Preservation exports the mailboxes, audit logs, sign in logs, rules, message traces and, where the counterparty cooperates, its tenant records, each hashed on acquisition. Analysis reconstructs the compromise timeline across both environments and names the first point at which the fraudulent instructions diverged from the original thread. Reporting puts that chronology in a document a treasurer, a claims adjuster and a judge can all read. Our business email compromise analysis practice has performed hundreds of compromised account analyses on this pattern.

When the matter moves toward litigation or an insurance claim, the report becomes a declaration or an affidavit, and the examiner who did the work signs it. Where the audit records are offered as business records, Federal Rule of Evidence 902(13) and 902(14) allow certification of records generated by an electronic process and of data copied from an electronic device through "a process of digital identification," which is why we hash every export at the time it is collected and document the tooling. Our examiners have testified in federal and state courts, and the report is written from the start as though it will be read aloud in a deposition, because in a disputed wire case it often is.

Insurers add a third audience. Crime and cyber policies often distinguish between social engineering losses and computer fraud losses, and the adjuster will ask whether an intruder was inside the insured's own systems or whether an employee was deceived into sending the payment voluntarily. The same tenant records that allocate fault between the companies answer that question, which is why we ask counsel early

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

whether a claim is contemplated so the report addresses the policy language in the order the adjuster will read it. Our banking industry financial fraud case study shows how a record assembled for one purpose served several, and the free initial consultation is the right time to raise the coverage question.

Preserve Your Email Containers and Cloud Logs Today

Inspect suspicious payment headers immediately in your browser using our zero upload Email Header Analyzer (evestigate.com/tools/email-header-analyzer/), read our guide to the first 24 hours of a business email compromise, and call Global Digital Forensics 24/7 at (800) 868-8189 to lock down your evidentiary record. The initial consultation is free.

Two Disputes Inside One Diverted Wire

The guide explains that a diverted wire hides two disputes, one with the bank under UCC Article 4A and one with the intended payee. This table separates them across the question each turns on, the record that answers it and what the examiner supplies, so counsel can see where the loss allocation is argued. Read the examiner column as the technical facts on the table. The security procedure framework governs the bank dispute, and comparative fault governs the one between the companies.

The bank dispute and the payee dispute in a diverted wire, what each turns on and the record behind it.

Dispute	Question it turns on	Record the examiner supplies
Sender against its bank	Whether a commercially reasonable security procedure was followed	Framed by UCC Article 4A, with the payment approval record as context
Sender against the payee	Which party's mailbox was compromised	Headers, audit logs and sign in records on each side
Where the message originated	The route and authorizing domain	Received chain, SPF, DKIM and DMARC results
Whether a tenant was accessed	Foreign sessions and rule changes	Audit log and Entra sign in records
When the thread was hijacked	The first divergence from the real thread	The timeline across both environments
Whether a lookalike domain was used	The impostor domain registration	Header analysis and registration records
Which policy clause applies	Social engineering against computer fraud	The same records read in the order the adjuster reads them

The banking industry case study shows examiners correlating email, deleted messages and documents with the institution's own records, the cross source reconciliation a diverted wire dispute requires.

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

Check the Payment Email Route in the Email Header Analyzer

In a disputed wire, each side should run its own copy of the fraudulent instruction through the Email Header Analyzer (evestigate.com/tools/email-header-analyzer/) and keep the results. Export the message as .eml or .msg, copy the complete header block and paste it in. The hop by hop Received chain shows whether the message originated inside the sender tenant, inside the recipient tenant or at a third party relay, and the SPF, DKIM and DMARC results show which domain actually signed it. Two parties reading the same header set side by side usually find the point where the thread left the genuine conversation. Nothing leaves your browser. Once the headers point at a compromised mailbox on either side, call so the audit logs are preserved while they are within retention.

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. Have the fraudulent message with full headers, the earlier genuine thread, the wire confirmation, the names of the mailboxes involved on both sides, and the licensing tier of your Microsoft 365 or Google Workspace tenant. The examiner will ask when the instructions changed, who verified them and how, whether a recall has been requested, whether counsel is engaged, and whether anyone has reset passwords or deleted rules since. You receive a scope that names the sources to preserve, a timing estimate for preservation and analysis, and a written proposal for counsel to approve. The initial consultation is free. Call (800) 868-8189 at any hour, or ask for our financial services team if the matter involves a bank or fund.

Technical References and Further Reading

Earlier reporting on this subject: FBI Internet Crime Complaint Center business email compromise warning, January 22, 2015 (archived copy).

Authorities cited in this guide: Uniform Commercial Code Article 4A, Funds Transfers. Defines security procedure and sets when a payment order is effective against the customer, as published in the Cornell LII text of the Uniform Commercial Code. FBI Internet Crime Complaint Center. Complaint intake for internet enabled fraud and the Recovery Asset Team that coordinates with banks on freezing transfers, as described on the IC3 site in 2026. Microsoft Purview audit log retention policies. Documents default and extended audit log retention periods for Microsoft 365, Microsoft Learn as read in October 2026. Federal Rule of Evidence 902. Items (13) and (14) permit certification of electronically generated records and hashed copies, Cornell LII text of the rule.

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

FREQUENTLY ASKED

Attribution in Wire Fraud Disputes

How fast must a wire recall be requested after a fraudulent transfer?

As soon as anyone suspects the beneficiary account is wrong. Recall is a request the bank makes on your behalf, and it works while funds remain in the receiving account, so speed matters because fraud operators move funds quickly through further transfers or cash withdrawals. Call the sending bank's fraud line first, give the wire reference and beneficiary details, then file a complaint with IC3 so the Recovery Asset Team can engage the beneficiary bank. Counsel should direct any written statement to the bank or counterparty. Preservation of mailboxes and logs runs in parallel with the recall.

Who is liable when a vendor's email is hacked and we paid the wrong account?

It depends on facts the record has to supply. If the fraudulent instructions came from inside the vendor's real tenant after its mailbox was taken over, the vendor's security failure is in play. If your own accounts payable mailbox had a hidden rule and the instructions were altered on your side, the analysis points the other way. Courts also weigh whether the payer verified the change through a known phone number and whether warning signs such as a lookalike domain were ignored. We examine which environment was compromised and when, and counsel argues the allocation from there.

Can you tell who sent the fraudulent payment instructions?

We can usually establish which account sent them, from what IP address and client, whether multi factor authentication was satisfied, and whether the session matches the account holder's normal pattern. Headers and DKIM results show whether a message truly left the claimed tenant or came from a lookalike domain. Identifying the person behind a stolen session combines those records with provider subpoenas and the work of law enforcement, and the report states which source supports each step.

How long are Microsoft 365 audit logs kept?

Microsoft documents a default retention of 180 days for audit records under standard licensing, with longer retention available under premium licensing and add ons, and Entra sign in and audit logs are retained for shorter periods that depend on the license. Google publishes its own retention table for Workspace log events. In practice the compromise often began before the window, so the sooner the export is taken the more of the record survives. Preservation is the first technical step in every wire fraud engagement for that reason.

What does a wire fraud attribution engagement cost and how long does it take?

Both depend on the number of mailboxes and tenants involved, whether the counterparty cooperates in producing its records, how far back the compromise reaches relative to retention windows, and whether the deliverable is a short attribution memo for an insurer or a declaration for litigation. The initial consultation is free, and after it you receive a written scope and proposal with the timing stated before work begins. The hotline at (800) 868-8189 answers 24/7, and preservation can begin before the proposal is signed when funds are at stake.

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

Web Addresses for the Sources Cited

1. FBI guidance on business email compromise: https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams/business-email-compromise
2. the FBI Internet Crime Complaint Center: https://www.ic3.gov/
3. UCC Article 4A: https://www.law.cornell.edu/ucc/4A
4. audit log retention page: https://learn.microsoft.com/en-us/purview/audit-log-retention-policies
5. 902(13) and 902(14): https://www.law.cornell.edu/rules/fre/rule_902
6. FBI Internet Crime Complaint Center business email compromise warning, January 22, 2015 (archived copy): https://web.archive.org/web/20161208011717/https://www.ic3.gov/media/2015/150122.aspx

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.