Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/resources/business-email-compromise-checklist/

EMERGENCY CHECKLIST

Business Email Compromise Checklist for Containment and Evidence Preservation

A diverted wire starts two clocks: the bank's recall window and your tenant's log retention. This checklist walks through what to freeze, who freezes it and what to hold as it is for the legal team and an examiner.

Why the First Hours Decide Both the Recall and the Record

A misdirected payment is discovered the same way almost every time. A vendor calls to ask where the money is, accounts payable pulls up the thread, and someone notices that the account change instructions came from an address one letter off from the real one. The funds are moving through the beneficiary bank and onward, so the recall request goes out first and fast. The technical record bearing on which mailbox was under someone else's control is preserved in the same hours: a capable administrator exports the rule, the sign in records and the messages first, then resets the password and removes the rule, which keeps the evidence the bank, the insurer and opposing counsel will ask for.

The reason the record matters is that a diverted wire produces two disputes at once. The first is between your company and its own bank, where the question under UCC Article 4A is whether the payment order was accepted under a commercially reasonable security procedure. The second is between you and the counterparty, where comparative fault turns on whose tenant was compromised and who missed the warning signs. Both questions are examined from logs that run on retention schedules set by the platform and the license, so the exports go first. Microsoft Entra sign in logs are retained for seven or thirty days depending on license, and the Purview unified audit log keeps 180 days under standard licensing. Our guide to the first 24 hours of a business email compromise explains the three parallel tracks. This checklist is the preservation track, written so you can run it tonight.

The Order of Operations, From the Bank Call to the Hash Log

The sequence starts with money, then evidence, because the recall window is the shortest clock in the building. The treasurer or controller who released the payment calls the sending bank's fraud desk with the reference number, the beneficiary account and the amount and asks for a recall and a freeze at the receiving institution. The same person, with counsel, files a complaint with the FBI Internet Crime Complaint Center so the Bureau can coordinate with the banks, and keeps a copy of exactly what was filed. While those calls are happening, the finance team keeps every message and record where it is. The payment approval emails, the vendor master change record, the call log showing whether anyone verified the new instructions by phone, and the original fraudulent messages are all part of the record, and each one bears on a question the bank and the insurer will ask.

Containment and evidence preservation run in parallel.

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

Who Acts, and Who Leaves the Mailbox to the Examiner

Authorized administrators block compromised sign ins and revoke sessions while GDF preserves mailbox rules, forwarding settings, messages and activity records. We hash the collected export files and document containment actions, operators and times in the response record.

Give the people most tempted to act a defined role in the plan. The question of what the intruder read is examined in the preserved MailItemsAccessed records, which keeps that trail free of new access entries attributed to the company. The fraudulent email stays in the mailbox for the examiner to collect, with its original headers and the route they record. And statements to the bank or the insurer about whether the company's systems were compromised are made once the record supports them, so every representation matches the forensic account that follows. Our wire fraud attribution guide explains how comparative fault is argued from exactly these records.

Cleanup Habits That Keep the Proof in Place

The first habit is exporting the rule before removing it. A hidden inbox rule that moved the vendor's replies to an obscure folder is strong evidence that your tenant, as well as the counterparty's, was accessed, and the export captures its creation timestamp, the creating session and the target folder. The second is saving the original message. A fraudulent message saved from the mailbox as received keeps the attacker's headers, where the examiner looks for a lookalike domain or a failed DMARC result. You can see what original headers contain with our Email Header Analyzer (evestigate.com/tools/email-header-analyzer/), which processes everything in your browser.

Two quieter habits matter as much. The first is bringing the counterparty in early. If the comparative fault argument turns on whose mailbox was compromised, the counterparty's sign in and rule records are half of the evidence, so the preservation request goes out the same day, inside their retention window. The second is scope. A compromise that began weeks before the fraudulent instruction may have touched more mailboxes than the one that sent the payment request, so the export covers every account in play while its logs are current. We recommend exporting sign in and audit records for every account the intruder's session touched, and expanding from there as the analysis identifies further sessions.

How GDF Supports Finance, Legal and Security Through the Analysis

Global Digital Forensics has analyzed hundreds of compromised accounts and collected thousands of mailboxes for law firms, insurers and corporate security teams since 1992. In a business email compromise we work alongside your administrators to capture the exports described above in a forensically sound and documented form, then analyze the headers, the authentication results, the inbox rule history and the sign in records to separate three propositions: that a fraudulent message arrived, that your tenant was accessed, and that the two are connected. Each proposition gets its own evidence in the report, so counsel can see the support behind each one and argue the allocation of loss on the ground the logs cover. Our business email compromise analysis and Microsoft 365 forensics pages describe the sources this draws on.

The deliverable is written for the people who lead the underlying inquiry. It contains a timeline with each event tied to its source record and its clock, a statement of the scope of what the record establishes, and, where needed, a declaration from the examiner who did the work. Finance receives the technical facts the IC3

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

complaint and the insurer's questionnaire ask for, in the same words used everywhere else. Our examiners have testified in federal and state courts, and the examiner who runs the analysis is the one who explains it. The first call is free, and it usually happens while the treasury team is still on the phone with the bank. Call (800) 868-8189 at any hour.

The Checklist at a Glance

The items to freeze in a business email compromise, who freezes each one, where it lives and how quickly it is gone.

Item	Who acts	Where it lives	How fast it expires
Wire recall request	Treasurer or controller with the sending bank fraud desk	Sending bank and beneficiary bank	Strongest in the first hours, while funds sit in the beneficiary account
IC3 complaint	Finance with legal, copy retained	FBI Internet Crime Complaint Center at ic3.gov	Most useful in the first hours, while funds can be traced
Microsoft Entra sign in logs	Global Administrator	Entra portal or SIEM export	Seven or thirty days by license
Unified audit log for affected users	Global Administrator or compliance administrator	Microsoft Purview audit search export	180 days standard, longer by license
Inbox rules, forwarding and delegates	Exchange administrator, export before removal	Exchange admin center or PowerShell export	Held until the rule is removed, so export comes first
Original fraudulent messages	Recipient, saved in place as received	Original .eml or .msg in the mailbox	Held as received while left in place
Google Workspace audit and login logs	Super Administrator	Admin console reports or export	About six months
Payment approvals and vendor master changes	Accounts payable lead	ERP change history and the approval mailbox	Held until the next vendor update

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

FREQUENTLY ASKED

Inbox Rules, Log Lifetimes and the Counterparty

Should we delete the malicious inbox rule right away?

Export it first. The rule's creation time, the session that created it and the folder it targets are evidence that your tenant was accessed, and the export captures all three. Pull the full rule and forwarding inventory for the affected mailbox, hash and log the export, and then remove the rule as a documented containment step. If the rule has already been removed, tell the examiner when and who removed it so the timeline accounts for it.

Can we forward the fraudulent email to counsel or to GDF?

Save the original instead. The original message is where the examiner reads the attacker's path, the Received chain, the authentication results and any lookalike domain evidence, and a forwarded copy carries your own path in their place. Save the original message from the mailbox as an .eml or .msg file, keep it in place and let the examiner collect it. Our Email Header Analyzer lets you read the original headers locally before anything is collected, and everything stays in the browser.

How long do the logs we need actually last?

It depends on the platform and the license. Microsoft Entra sign in logs are retained for seven or thirty days by license, the Purview unified audit log keeps 180 days under standard licensing and longer with premium licensing, and Google Workspace audit records are retained for about six months. Inbox rules and forwarding settings are held only while they exist, so they are exported before anyone removes them. Export in that order, shortest window first.

Does the counterparty have to preserve anything?

Counsel can ask them to, and should, the same day. If the dispute turns on whose mailbox was compromised, the counterparty's sign in logs, rule history and original messages are half of the record. A short preservation letter costs little and makes the comparative fault argument fair when it is made months later. The legal team decides each next step with the counterparty, and we document what was requested and when.

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.