EVIWRITE INSIGHT BRIEFING

INSIGHTS & EVIDENTIAL BRIEFING

Controlled EviWrite publication generated from the article's Markdown source and structured evidential metadata.

DOCUMENT SERIES	Cyber Evidence and Incident Records
USE CASE	cyber-incident-evidence
STATUS	Published
REFERENCE	EW-INSIGHT-THE-BEC-EVIDENCE-GAP

PUBLICATION TITLE

The BEC Evidence Gap: Why Payment Fraud Is Not Just an Email Problem

Business Email Compromise is often treated as a phishing failure. The deeper failure is evidential: the organisation cannot prove why a fake instruction became an authorised payment.

Published 2026-02-21 Updated 2026-05-25 Reviewed 2026-05-25

EVIWRITE INSIGHT PUBLICATION RECORD

The BEC Evidence Gap: Why Payment Fraud Is Not Just an Email Problem

Business Email Compromise is often treated as a phishing failure. The deeper failure is evidential: the organisation cannot prove why a fake instruction became an authorised payment.

CANONICAL URL	https://eviwrite.com/insights/the-bec-evidence-gap/
PDF DOWNLOAD	https://www.eviwrite.com/downloads/insights/the-bec-evidence-gap.pdf
CATEGORY	cyber-incident-evidence
SERIES	Cyber Evidence and Incident Records
SERIES PART	3
SERIES LABEL	Business email compromise evidence
READING LEVEL	Professional
REVIEW STATUS	Reviewed by EviWrite
AUTHOR	EviWrite - Independent Evidential Authority
REVIEWER	EviWrite - Independent Evidential Authority
OWNER	EviWrite
PUBLISHED	2026-02-21
UPDATED	2026-05-25
REVIEWED	2026-05-25
REFERENCE	EW-INSIGHT-THE-BEC-EVIDENCE-GAP
SUGGESTED CITATION	EviWrite, "The BEC Evidence Gap: Why Payment Fraud Is Not Just an Email Problem," EviWrite Insights, 2026.

TAGS

business email compromise | BEC evidence | payment fraud | funds transfer fraud | invoice fraud | supplier fraud | cyber insurance | payment controls

KEYWORDS

business email compromise evidence | BEC evidence gap | payment fraud evidence | funds transfer fraud evidence | supplier bank account change evidence | invoice redirection fraud evidence | cyber insurance BEC claim evidence | business email compromise controls | payment approval evidence | vendor master evidence

EviWrite evidential boundary

This publication is a public evidential analysis document. It records sources, interpretation limits, article metadata, review history, and evidence boundaries. It does not determine liability, coverage, compliance, recoverability, or legal responsibility in any specific incident.

Jurisdiction note

This article discusses general evidential, cyber, finance, insurance, governance, and incident-response issues around Business Email Compromise, payment diversion fraud, and funds transfer fraud. It references UK and US materials where useful, but it is not jurisdiction-specific legal, insurance, banking, regulatory, or cyber-response advice.

Advice disclaimer

This article is general evidential analysis, not legal advice.

Record scope

Business Email Compromise, payment diversion fraud, supplier bank-detail changes, payment authority, verification records, cyber claims, supplier disputes, and recovery evidence.

Proof boundary

This article records general evidential analysis and source-based commentary. It does not determine liability, insurance coverage, recoverability, regulatory compliance, cyber-response sufficiency, or legal responsibility in any specific BEC incident.

EXECUTIVE BRIEF

The argument in one page

Core thesis

Business Email Compromise is often treated as a phishing failure. The deeper failure is evidential: the organisation cannot prove why a fake instruction became an authorised payment.

01 **BEC does not succeed because one email is convincing. It succeeds because the organisation's own systems treat the fake instruction as a real business decision.**

02 **The missing record is usually not the email. It is the evidence chain between supplier identity, bank-detail change, approval, callback, payment release, bank transfer, and recovery action.**

03 **Serious payment evidence must exist before money moves. After payment, the organisation is no longer proving control. It is explaining failure.**

Minimum defensible record

Instruction | Identity and source | Authority | Verification | Payment pathway | Proof boundary

Why it matters

Serious readers do not only ask whether an event happened. They ask what record survived, when it was created, who relied on it, what it proves, and where its limits are.

CONTENTS

Briefing structure

DOCUMENT CONTROL

Controlled publication metadata

TITLE	The BEC Evidence Gap: Why Payment Fraud Is Not Just an Email Problem
REFERENCE	EW-INSIGHT-THE-BEC-EVIDENCE-GAP
CANONICAL URL	https://eviwrite.com/insights/the-bec-evidence-gap/
PDF DOWNLOAD PATH	/downloads/insights/the-bec-evidence-gap.pdf
PDF SIDECAR PATH	/downloads/insights/the-bec-evidence-gap.pdf.json
SOURCE FILE	content/insights/the-bec-evidence-gap.md
GENERATOR	eviwrite-md-yaml-pdf-v6-public-downloads
GENERATED	2026-06-11T13:06:58.064Z
PUBLISHED	2026-02-21
UPDATED	2026-05-25
REVIEWED	2026-05-25
STATUS	published

PDF SHA-256 is written after generation to the sidecar file: **/downloads/insights/the-bec-evidence-gap.pdf.json**.

QUICK READ

Executive summary

01 **BEC does not succeed because one email is convincing. It succeeds because the organisation’s own systems treat the fake instruction as a real business decision.**

02 **The missing record is usually not the email. It is the evidence chain between supplier identity, bank-detail change, approval, callback, payment release, bank transfer, and recovery action.**

03 **Serious payment evidence must exist before money moves. After payment, the organisation is no longer proving control. It is explaining failure.**

FIVE LINES THAT DEFINE THE ARGUMENT

Core evidential framing

01

BEC does not succeed because one email is convincing. It succeeds because the organisation’s own controls agree to behave as if the email is true.

EviWrite - A concise framing line for the evidential failure behind Business Email Compromise and payment diversion fraud.

02

The fraudster sends the instruction. The business supplies the authority.

EviWrite - A sharp governance quote explaining why BEC is a payment-authority problem, not only an email-security problem.

03

A callback made to the number inside the suspicious email is not a control. It is customer service for the attacker.

EviWrite - A warning about control theatre in supplier and payment verification.

04

The invoice was fake. The approval was real. That is why the evidence matters.

EviWrite - A practical quote for finance, procurement, cyber, insurance, legal, and board readers.

05

If your payment trail only proves that your own workflow said yes, it proves the fraud entered the business with permission.

EviWrite - A warning against treating internal approval logs as proof of independent verification.

ARTICLE BODY

01

The email is not the incident

Business Email Compromise looks like an email problem.

That is why so many organisations misread it.

A fake supplier message arrives. A compromised mailbox sends a believable instruction. An executive appears to request an urgent payment. A finance team receives new bank details. A vendor record is changed. An invoice is approved. A payment batch is released. Money leaves.

The email matters.

But the email is not the whole incident.

The real incident is the conversion of a suspicious instruction into authorised business action.

That is where most BEC evidence fails. Organisations preserve the email, the invoice, the bank confirmation, and the workflow approval, then assume they have the incident file. They do not. They have fragments from the beginning and end of the fraud. The critical missing record sits in the middle: why did the organisation decide the instruction was real?

The FBI describes Business Email Compromise as one of the most financially damaging online crimes, and its 2024 IC3 report recorded more than $2.77 billion in reported BEC losses. The NCSC describes business payment fraud as criminals tricking organisations through tailored emails, including requests to pay into a different bank account. Those definitions are useful. They still do not answer the evidential question.

The deeper question is not whether the message was fake.

The deeper question is why the organisation's own systems accepted it.

"BEC does not succeed because one email is convincing. It succeeds because the organisation's own controls agree to behave as if the email is true."

That is the evidence gap.

02

The real failure is trust conversion

> **The fraudster sends the instruction. The business supplies the authority.**

Most businesses split BEC across several teams.

Cyber looks at spoofing, compromised accounts, headers, phishing, malware, MFA, and mailbox rules. Finance looks at invoice approval, supplier records, payment batches, bank release, and reconciliation. Procurement looks at vendor onboarding and supplier changes. Legal looks at liability, notification, privilege, recovery, and insurance. The board asks how the payment got through.

Everyone owns a piece.

Nobody owns the evidential chain.

That is why BEC is so destructive. It crosses the seam between communication, identity, authority, verification, approval, and money movement. Attackers do not need to defeat every control. They need to make the control environment behave as if the request is ordinary.

They use urgency, hierarchy, familiarity, supplier relationships, payment timing, end-of-month pressure, executive travel, tender deadlines, and ordinary reluctance to slow down a transaction that appears commercially normal.

Sometimes the fake invoice sounds like the supplier because the attacker has read the real conversation.

Sometimes the payment change arrives exactly when the accounts team expects one.

Sometimes a compromised mailbox watches correspondence until the right moment.

Sometimes a senior-person request is shaped to make verification feel disloyal.

The fraudster sends the instruction.

The business supplies the authority.

03

The missing record is payment authority

After a BEC incident, organisations often have proof that a payment happened.

That is not the same as proof that controls worked.

The missing record is the payment-authority record. It should answer one question: what made this instruction trustworthy enough to act on?

That record should connect the source request, supplier identity, bank-detail change, previous supplier data, independent verification, contact route, approver authority, exception logic, payment release, and decision boundary.

Most businesses cannot produce that record cleanly.

They can show an approval log. They can show that an authorised user clicked a button. They can show the invoice entered the payment run. They can show the supplier record was changed. They can show the bank transfer. Those facts matter, but they often prove only that the internal workflow executed.

They may not prove independent judgement.

A workflow approval may show that the fraud successfully entered the system and received a legitimate internal blessing. It may not show that anyone checked the thing that actually mattered.

Was the supplier change genuine?

Was the number used for callback independently sourced?

Was the person contacted actually authorised?

Was the request consistent with previous supplier behaviour?

Was the approver shown the risk signal?

Was the exception recorded?

Was the payment held pending independent confirmation?

If the evidence cannot answer those questions, the organisation should expect further challenge from banks, insurers, suppliers, auditors, boards, or investigators.

The invoice was fake. The approval was real. That is why the evidence matters.

04

The callback must escape the compromised channel

Most BEC guidance says organisations should verify payment requests through a second channel.

That is correct.

It is also incomplete.

A callback is only as strong as the evidence around it. The business needs to show what number was used, where the number came from, who made the call, who answered, what was confirmed, what was not confirmed, what documents or details were checked, whether there were discrepancies, and who decided the result was enough.

The weakest callback is the one made to the number supplied inside the suspicious email.

That is not independent verification. That is asking the attacker to confirm the attack.

“A callback made to the number inside the suspicious email is not a control. It is customer service for the attacker.”

A stronger callback uses a pre-existing trusted source: a verified supplier master record, contract file, official website, prior independently verified contact, or separate trusted channel. Even then, the evidence should preserve the route used and the result of the conversation.

The same applies to video calls, messaging apps, supplier portals, and meeting links. Attackers can compromise mailboxes, imitate writing styles, intercept real threads, create convincing domains, and exploit existing trust. The verification record must therefore prove more than “someone checked.”

It must show how the check escaped the compromised channel.

05

Supplier bank-detail changes are evidence events

A supplier bank-detail change should not be treated as routine administration.

It is one of the highest-risk evidence moments in the finance system.

The organisation should preserve the request, source channel, previous bank details, proposed new details, effective date, supplier identity check, independent callback, approver, exception path, payment hold, and confirmation record. It should also preserve the reason the change was accepted and the timing of the first payment

after change.

Most organisations under-record this moment.

They treat the supplier master as an operational record: a place where data is updated so payment can continue. That is not enough. The supplier master is also a future evidence file. If money is diverted, the first question will be how the new bank details became trusted.

The supplier-change record should be harder to fake than the supplier-change request.

That requires separation. The person receiving the request should not be the only verification point. The new bank details should not become active merely because an email asked for them. The first payment after change should not move without heightened evidence. Emergency changes should create more proof, not less.

Fraud loves urgency because urgency makes weak evidence feel efficient.

A proper supplier-change record slows down only the dangerous part: the leap from communication to authority.

06

ERP approval is not independent verification

> **The invoice was fake. The approval was real. That is why the evidence matters.**

ERP systems, procurement workflows, finance platforms, email logs, security alerts, bank confirmations, and supplier-master histories can all generate useful records.

They are not proof of truth by themselves.

A workflow log may show that a step was completed by a named user. It may not show what the user saw, what they understood, what risk signal was available, what verification occurred, or whether the approval was based on genuine authority.

A supplier-master record may show that bank details changed. It may not show that the change was genuine.

A payment confirmation may show that funds were sent. It may not show recoverability, liability, policy cover, or control sufficiency.

This distinction matters after BEC.

The organisation may say the payment was approved according to process. The insurer, bank, auditor, supplier, or board may ask a different question: did the process verify the thing that mattered?

An approval process that does not force independent verification of new bank details is not a payment control. It is a payment conveyor belt with manners.

This is the control-theatre problem inside BEC. The system produces a respectable-looking trail. The trail shows that the wrong action moved through the right workflow. That may be administratively neat. It is evidentially weak.

If your payment trail only proves that your own workflow said yes, it proves the fraud entered the business with permission.

07

BEC exploits hierarchy, not just technology

BEC is often described as social engineering.

That phrase is accurate, but too shallow.

The attack exploits the hierarchy of the business. A junior finance employee may hesitate to challenge a CFO. A procurement manager may avoid annoying a key supplier. An accounts-payable team may not want to delay a time-sensitive payment. A project lead may not want to disrupt a closing date. A charity, school, publisher, agency, or public body may have thin staffing and a strong culture of helpfulness.

The attacker turns normal business behaviour into a control weakness.

BEC is not only about gullible people clicking bad emails. It is about organisations that reward speed, politeness, hierarchy, and commercial smoothness more consistently than they reward verification.

A finance team may know the policy.

The team may also know that slowing down a senior request creates friction.

That is why evidence design matters. A good control should make the right behaviour easier to defend. The employee who pauses a payment should have a record-backed process to stand on. The approver should see the evidence gap before approval. The system should require the independent number source, not merely a tick box saying “verified.”

Verification should not depend on personal courage.

It should be built into the payment evidence record.

08

After payment, timing becomes evidence

Once money moves, the recovery clock becomes evidence.

The organisation must show when the fraudulent instruction was received, when the payment was approved, when funds were released, when the fraud was discovered, when the bank was contacted, what recall request was made, what receiving account was identified, when law enforcement or fraud-reporting bodies were notified, and what instructions were received.

Timing can affect recovery prospects, insurer assessment, legal responsibility, bank action, and post-incident review.

The FBI advises victims of internet crime to notify all financial institutions involved in the relevant transactions, submit an IC3 complaint, contact the nearest FBI field office, and contact local law enforcement. The NCSC similarly advises organisations tricked into fraudulent payments to report internally and contact the bank directly

using official details.

The evidence point is direct: speed must be recorded.

A business that waited two hours may still have acted reasonably. A business that cannot show when it discovered the fraud and when it contacted the bank has created a new problem.

The recovery trail should be preserved like the payment trail.

Bank contact. Call reference. Recall request. Fraud report. Account freeze attempt. Receiving bank details. Law-enforcement report. Insurer notice. Customer or supplier communication. Internal escalation. Board update. Remediation decision.

After payment, every hour becomes part of the file.

09

Insurance, supplier disputes, and recovery all depend on the chain

BEC creates classification problems.

Is the loss business email compromise? Funds transfer fraud? Social engineering fraud? Cybercrime? Computer fraud? Crime policy? Cyber policy? Invoice fraud? Supplier fraud? Employee error? Voluntary transfer? A sub-limited event? A policy exclusion?

Those distinctions can affect cover, limits, exclusions, notification duties, recovery expectations, cooperation obligations, and claim handling.

The evidence record needs to show not only that a loss occurred, but how the loss occurred. That means connecting the fraudulent communication to the internal action and the resulting payment. It also means showing policy-relevant facts: whether an account was compromised, whether credentials were used, whether systems were accessed, whether the instruction came from a spoofed domain, whether a supplier was impersonated, whether an employee released payment, whether verification controls were required, and whether those controls operated.

A weak claim says: we were tricked and lost money.

A stronger claim shows the pathway from deception to authority to transfer.

BEC can also create a second conflict. The business thought it paid the supplier. The supplier never received funds. The supplier still wants payment. The business says it acted on what appeared to be supplier instructions. The supplier says its genuine payment details never changed.

That dispute turns on evidence.

Who controlled the compromised mailbox? Which party received the fake instruction? Who changed the bank details? What verification was required by contract? What route was used? Which contact details were trusted? Were payment terms altered? Did the supplier warn about fraud? Did the business follow its own controls? Did either side notice a changed domain, unusual wording, altered invoice format, new account name, or timing inconsistency?

This is where BEC stops being a cyber story and becomes a commercial evidence dispute.

The contract can define the supplier-payment protocol.

The evidence record must show whether it happened.

10

The evidence should exist before the attack

The best BEC evidence is not created after the loss.

It is built into the payment process before the attacker arrives.

That means treating certain events as evidence events: new supplier onboarding, supplier bank-detail change, high-value payment, first payment after change, urgent executive request, payment outside normal pattern, payment to new geography, payment to a new account name, exception approval, and payment release after failed verification.

Each event should create a record that survives outside the compromised channel.

The question is not whether the organisation has a policy. Most do. The question is whether the organisation can prove the policy operated in the specific payment.

That requires more than a tick box.

It requires independent contact-source evidence, previous and new payment-detail record, approval context, risk flag visibility, exception rationale, segregation-of-duty proof, payment hold or release record, and proof boundary.

Better email security helps. Phishing training helps. MFA helps. Bank controls help.

But BEC lives in the handoff between message and money.

The control record must live there too.

The attack begins in communication.

The loss happens in authority.

11

A practical BEC evidence protocol

A serious protocol is not complicated. It is disciplined.

- Treat every supplier bank-detail change, first payment after change, urgent executive payment request, and payment outside normal pattern as a high-risk evidence event.
- Require independent verification using a trusted contact source that did not arrive through the suspicious instruction.
- Preserve the source request, previous supplier details, proposed new details, contact-source evidence, verification outcome, approver, exception reason, payment release, bank confirmation, and proof boundary.

- Give finance staff explicit authority to pause payment without being punished for delaying convenience.
- Preserve recovery evidence immediately after discovery: bank contact, recall request, fraud report, insurer notice, law-enforcement report, supplier communication, and board escalation.

The EviWrite position is simple: a payment-control record should not merely show that a payment was processed. It should show why the organisation was entitled to trust the instruction at the moment authority was given.

That means preserving the evidence of identity, verification, approval, exception handling, payment release, recovery action, and proof limits as a structured record, not as scattered screenshots after the loss.

12

Public proof does not require exposing payment data

BEC records will often contain sensitive material: supplier details, bank accounts, email headers, employee names, legal advice, insurer communications, fraud reports, internal control findings, and recovery steps.

That does not mean the evidence cannot be structured.

A serious evidential model separates private substance from proof layer. The private record preserves the sensitive material. The proof layer records existence, timing, status, chain, verification action, and evidence boundary without exposing payment details unnecessarily.

This matters after fraud.

The business may need to show an insurer, bank, auditor, supplier, regulator, board, or investigator that a record existed at a certain time, that a supplier-change evidence file was created, that callback verification was recorded, that payment release was linked to approval, or that recall action occurred promptly.

That can be done without making supplier bank details public.

Public proof does not mean public exposure.

It means the record can be checked without relying only on memory, screenshots, compromised inboxes, or internal confidence.

13

The future of BEC defence is evidence, not awareness

> **If your payment trail only proves that your own workflow said yes, it proves the fraud entered the business with permission.**

Most post-incident reviews ask how the email got through.

That question matters.

The better question is: how did the business turn that email into authority?

Which system accepted the instruction? Which person relied on it? Which control was supposed to challenge it? What evidence did the approver see? What independent source was used? What exception was created? Why was payment released? What record survived? What was missing?

That is the question that makes BEC less mysterious.

Awareness training will remain useful.

Email security will remain useful.

MFA will remain useful.

Bank controls will remain useful.

But none of them solves the deeper evidence problem alone.

BEC is a business-decision attack. It uses communication to corrupt authority. The defence must therefore record authority with the same seriousness that security teams record intrusion.

The organisation that can prove its payment controls worked, or prove exactly where they failed, is in a stronger position with banks, insurers, suppliers, auditors, boards, and investigators. The organisation that can only produce the fake email and the transfer receipt is already fighting from a weaker place.

The next serious payment-control standard will not be “did someone approve it?”

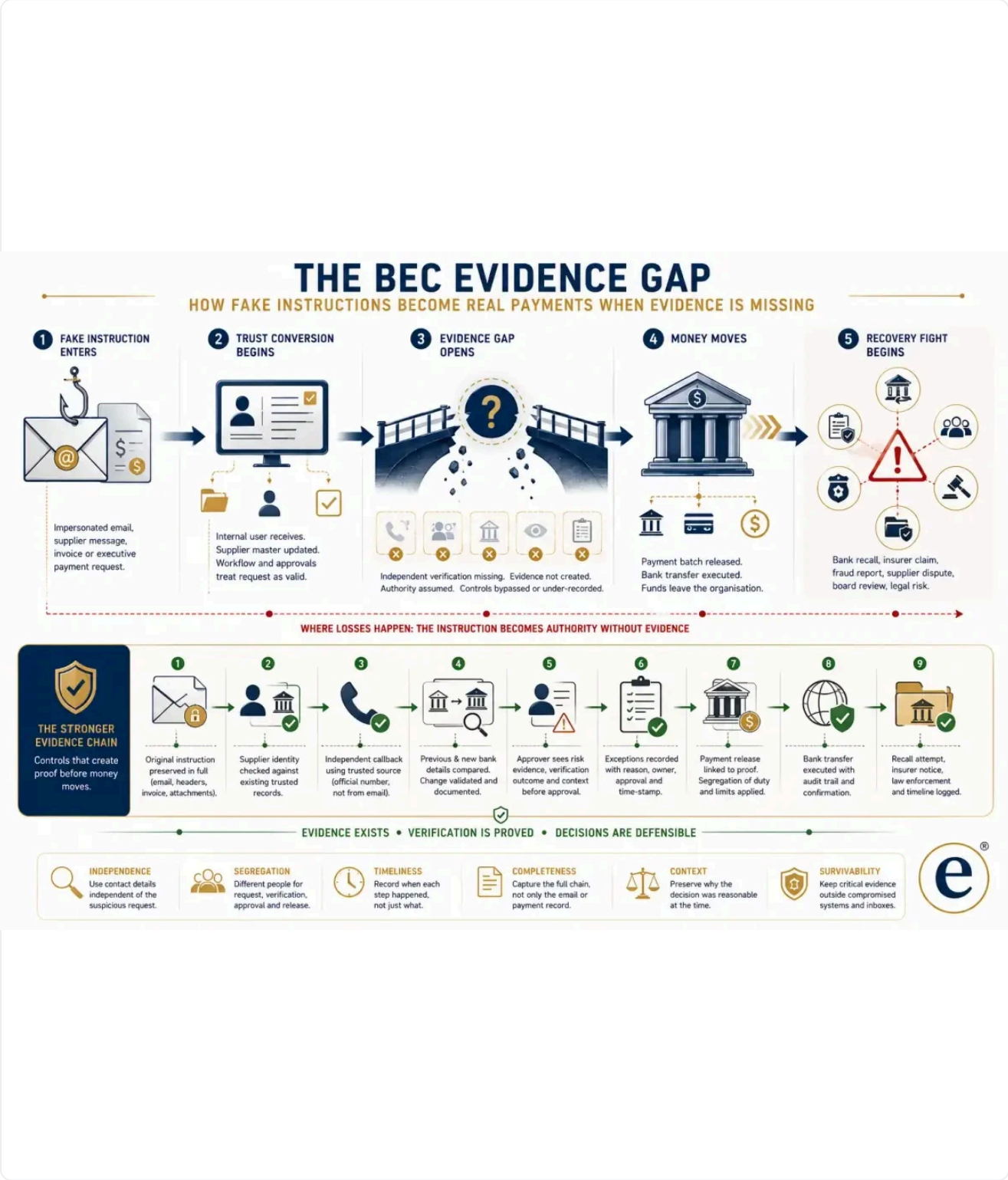
It will be “what evidence made approval reasonable?”

Do not wait until the money is gone.

Show why the payment was trusted before the money moves.

EXHIBIT A

The fake payment evidence chain



BEC evidence must connect the fake instruction to the internal business decisions that allowed money, data, or authority to move. The infographic includes the EviWrite Evidential Mark in the bottom-right corner.

EXHIBIT A TRANSCRIPT

The fake payment evidence chain

The infographic shows how a fraudulent instruction becomes a real payment when controls produce authority without preserving evidence.

- Stage one: impersonation — spoofed email, compromised mailbox, fake supplier request, executive instruction, invoice redirection, or altered bank details.
- Stage two: trust conversion — internal staff, workflow tools, supplier records, approval systems, and payment controls convert the request into authorised action.
- Stage three: evidence gap — missing independent callback, missing number source, missing authority boundary, missing supplier-change proof, missing exception rationale, and missing verification record.
- Stage four: recovery fight — bank recall, insurer claim, supplier dispute, law-enforcement report, board review, customer communication, and post-incident control remediation.
- EviWrite Evidential Mark — a small visible circled e with the words 'EviWrite Evidential Mark' appears in the bottom-right corner of the infographic.

EVIWRITE POSITION

Two controls the record must prove

EVIDENCE GAP

The fraudster sends the instruction. The business supplies the authority.

BEC becomes expensive when a fake message is converted into an internal approval, supplier change, payment release, or exception that later cannot be properly evidenced.

Read how verification boundaries work
https://www.eviwrite.com/verification/

PAYMENT AUTHORITY

The callback is not enough if the callback cannot be proved.

A serious payment-control record should show who verified the request, what independent contact source was used, what was confirmed, what changed, who approved the exception, and what evidence survived.

Read how EviWrite Evidencing works
https://www.eviwrite.com/evidencing/

PROOF LIMITS

What this type of record can and cannot show

Can support

- That identified BEC-related instructions, payment records, supplier changes, approval steps, callbacks, bank actions, fraud reports, or recovery steps were recorded at a stated time.
- That specified evidence sources were used to assess authenticity, authority, payment causation, control operation, insurer notice, recovery action, or supplier responsibility where captured.
- That a structured evidential pathway exists for explaining BEC-related claims to banks, insurers, boards, suppliers, customers, auditors, or investigators.
- That the record's evidential scope, unknowns, assumptions, and verification boundary have been defined rather than implied.

Does not prove

- That the payment was lawful, recoverable, insured, or authorised merely because internal workflow approved it.
- That a callback was independent unless the record shows the source of the contact route and what was verified.
- That the supplier, bank, employee, customer, insurer, or platform is automatically liable.
- That every compromise, account access, communication, or internal failure has been identified unless the record specifically supports that conclusion.

A BEC evidence record is strongest when it separates the fake external instruction from the genuine internal actions that gave it force. It should not be used to overclaim recoverability, liability, insurance cover, lawful authority, control sufficiency, or absence of compromise.

TOOL 1

EVIWRITE FRAMEWORK

The BEC payment-evidence chain

A defensible BEC record connects the suspicious instruction to the internal decision pathway that changed supplier data, approved payment, released funds, and triggered recovery action.

STEP	EVIDENCE FUNCTION	RECORD REQUIREMENT
01	**Instruction**	Preserve the email, message, invoice, attachment, account-change request, phone note, meeting record, or supplier communication that initiated the action.
02	**Identity and source**	Record whether the sender, domain, account, supplier, executive, phone number, bank details, and payment request were independently verified.
03	**Authority**	Show who had authority to change supplier records, approve the payment, override controls, release funds, or accept an exception.

STEP	EVIDENCE FUNCTION	RECORD REQUIREMENT
04	**Verification**	Record the callback method, independent number source, person contacted, confirmation given, verification questions, and any discrepancy or uncertainty.
05	**Payment pathway**	Connect supplier-master change, invoice approval, payment batch, bank instruction, value date, release time, receiving account, recall attempt, insurer notice, and law-enforcement report.
06	**Proof boundary**	State what the record proves, what it merely supports, what was not checked, what remains unknown, and what should not be inferred from internal approval alone.

TOOL 2

PRACTICAL CHECKLIST

Evidence to preserve before and after BEC

The useful BEC record is not the fake email alone. It is the chain showing how identity, authority, verification, approval, payment release, and recovery were handled.

NO.	EVIDENCE ITEM	WHAT TO PRESERVE	WHY IT MATTERS
01	**Original instruction.**	Preserve the email, full headers where available, attachment, invoice, reply chain, message record, caller note, payment request, or bank-detail change request.	Shows what triggered the business action instead of relying on a later summary of the fraud.
02	**Identity context.**	Record who or what was being impersonated: supplier, customer, executive, employee, domain, mailbox, phone number, payment account, or previous relationship.	Separates the apparent sender from the verified business identity.
03	**Supplier-change history.**	Preserve the vendor-master or supplier-record history showing previous details, proposed new details, who changed them, when, why, and under which approval route.	Shows how a fake instruction became trusted payment data.
04	**Independent verification.**	Record the callback route, the independent source of the number or contact method, who made contact, who responded, what was confirmed, and what remained uncertain.	Proves the check escaped the suspicious channel instead of asking the attacker to verify the attack.
05	**Authority and approval.**	Preserve approver identity, authority basis, segregation-of-duty checks, exception approvals, override reasons, payment hold decisions, and risk warnings shown to the approver.	Shows whether approval was meaningful or just workflow theatre.
06	**Payment pathway.**	Connect invoice approval, supplier change, payment batch, bank instruction, value date, release time, receiving account, transfer confirmation, and payment reference.	Links the fraudulent instruction to the actual movement of money.
07	**Discovery and recovery timeline.**	Record discovery time, bank contact time, recall request, fraud report, insurer notice, law-enforcement report, supplier or customer communications, and recovery outcome.	Preserves the speed and quality of the response after money moved.

NO.	EVIDENCE ITEM	WHAT TO PRESERVE	WHY IT MATTERS
08	**Control-operation record.**	Separate the fake external instruction from the genuine internal actions that accepted it, including checks performed, checks missed, controls bypassed, exception reasons, and pressure points.	Makes the review useful instead of reducing BEC to blame or phishing awareness.
09	**Proof boundary.**	State what the record proves, what it only supports, what was not checked, what remains unknown, and what should not be inferred from internal approval alone.	Prevents the organisation from overclaiming recoverability, liability, insurance cover, or lawful authority.

Golden rule: Do not let a payment move because a workflow said yes. Preserve the evidence that made the yes reasonable.

TOOL 3

WEAK PAYMENT RECORDS VERSUS STRONGER BEC EVIDENCE

Where BEC evidence quietly collapses

Many organisations can show that a payment was approved. Fewer can show why a fraudulent instruction was trusted.

WEAK RECORD	MAY SHOW	MAY NOT SHOW	STRONGER APPROACH
Suspicious email	The apparent instruction, sender, attachment, wording, or payment request	Why the business accepted it, who verified it, or whether the channel was compromised	Preserve the full instruction with headers, account context, supplier history, verification records, and decision trail
ERP approval log	That a workflow step was completed by an authorised user	Whether independent verification occurred or whether the approver saw the relevant risk	Link approval to evidence reviewed, verification method, exception handling, authority boundary, and payment release
Callback note	That someone claims a call was made	Whether the number was independently sourced, who answered, what was confirmed, or whether the call proved anything	Record independent number source, caller, recipient, confirmation questions, outcome, timestamp, and proof limits
Supplier bank-detail change	That vendor records were updated	Whether the change request was genuine, authorised, verified, or linked to the correct supplier	Maintain a supplier-change evidence record with source request, independent verification, approval, previous details, new details, and effective date
Bank transfer confirmation	That funds were sent	Whether the payment was authorised by a genuine business instruction or recoverable after fraud discovery	Connect transfer evidence to recall action, bank contact, receiving account details, fraud report, insurer notice, and recovery timeline

COMMON FAILURE PATTERNS OBSERVED IN WEAK EVIDENCE RECORDS

COMMON MISTAKES

How businesses help BEC evidence fail

The biggest BEC evidence failures are not technical. They are control records that look respectable until someone asks what they actually verified.

01 Treating the fake email as the incident instead of examining the internal authority chain that made the fake instruction executable.

02 Calling a number supplied in the suspicious email, invoice, footer, or attachment and recording the call as independent verification.

03 Failing to record the source of the trusted contact details used for verification.

04 Treating ERP approval as proof of verification when it only proves that a workflow accepted the request.

05 Changing supplier bank details without preserving the source request, previous details, independent confirmation, approval, and effective date.

06 Allowing urgent, confidential, senior, or relationship-preserving requests to bypass the evidence standard.

07 Preserving the payment record but not the decision record that allowed payment.

08 Waiting until the bank, insurer, customer, supplier, or board asks for proof before building the incident file.

WHAT THIS MEANS FOR

Audience implications

Businesses

Businesses need BEC evidence that links email, supplier records, approvals, callbacks, bank transfers, insurer notices, recovery actions, and control-operation records into one coherent incident file.

Legal and compliance

Legal teams need records that separate the fake instruction, genuine internal approval, control operation, contractual duties, bank action, privilege boundaries, recovery evidence, and unresolved liability questions.

Providers

Finance, procurement, cyber, email-security, ERP, banking, and workflow providers should preserve exportable proof of verification, not only activity logs or dashboard status.

AI teams

AI teams using automated invoice processing, payment approval, supplier screening, or fraud detection should preserve why an instruction was trusted, not only what the model or workflow decided.

Public institutions

Public institutions need payment-fraud records that show accountable process, independent verification, exception handling, recovery action, and public-money stewardship without exposing sensitive security details.

Education and research

Schools, universities, and research bodies handling grants, suppliers, bursaries, donations, research payments, or international vendors should preserve supplier-change and payment-verification records before funds move.

RELATED EVIWRITE DOCTRINE

Further evidential guidance

Evidencing

Create structured records before payment, supplier, and cyber incident claims are challenged.

https://www.eviwrite.com/evidencing/

Verification

Understand how bounded verification helps others check a claim without exposing sensitive payment or supplier data.

https://www.eviwrite.com/verification/

Ransomware Evidence

Read how ransomware evidence must survive operational disruption, data compromise, recovery claims, and insurer scrutiny.

https://www.eviwrite.com/insights/ransomware-evidence-before-encryption/

The Control Theatre Problem

See why governance controls fail when leaders receive assurance without source evidence.

https://www.eviwrite.com/insights/the-control-theatre-problem-why-compliance-evidence-fails-inside-the-hierarchy/

APPENDIX — EVIWRITE EVIDENCE NOTE

Evidence record for this article

Sources, boundaries, citation details, review history, and machine-readable notes showing how this article should be interpreted.

ARTICLE	The BEC Evidence Gap: Why Payment Fraud Is Not Just an Email Problem
REFERENCE	EW-INSIGHT-THE-BEC-EVIDENCE-GAP
CANONICAL PATH	/insights/the-bec-evidence-gap/
STATUS	published
REVIEWED	2026-05-25

A1 — SOURCE GROUPS

Sources behind the argument

Business Email Compromise and payment fraud

S01 — Business Email Compromise

Publisher: Federal Bureau of Investigation

https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise

Used to ground the article’s treatment of BEC as one of the most financially damaging online crimes and as a fraud exploiting trusted business communication.

S02 — 2024 IC3 Annual Report

Publisher: Federal Bureau of Investigation Internet Crime Complaint Center

https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Used to support the article’s discussion of BEC losses, financial fraud reporting, and the importance of timely reporting to banks, IC3, FBI field offices, and law enforcement.

S03 — Business Email Compromise: The $55 Billion Scam

Publisher: Federal Bureau of Investigation Internet Crime Complaint Center

https://www.ic3.gov/PSA/2024/PSA240911

Used to support the article's view that BEC has evolved into a global, high-loss fraud category involving exposed losses and increasingly sophisticated techniques.

S04 — Business payment fraud

Publisher: National Cyber Security Centre

https://www.ncsc.gov.uk/section/respond-recover/ml-business-payment-fraud

Used to inform the article's discussion of fraudulent payment requests, invoice redirection, reporting to IT, contacting the bank directly, and using official contact routes.

S05 — Payment diversion fraud

Publisher: Report Fraud / City of London Police

https://www.reportfraud.police.uk/payment-diversion-fraud/

Used to support the article's treatment of spoofing, urgency, altered payment instructions, executive or supplier impersonation, secondary verification, multi-person approval, and financial-institution notification.

Cyber claims, insurance, and financial recovery

S06 — 2025 Cyber Claims Report

Publisher: Coalition

https://web.coalitioninc.com/download-2025-cyber-claims-report.html

Used as a market reference for BEC and funds transfer fraud claims activity.

S07 — Business email compromise tops cyber claims: Coalition

Publisher: Business Insurance

https://www.businessinsurance.com/business-email-compromise-tops-cyber-claims-coalition/

Used to support the article's treatment of BEC as a leading cyber incident type in claims reporting.

Controls, identity, logs, and evidence

S08 — SP 800-92: Guide to Computer Security Log Management

Publisher: National Institute of Standards and Technology

https://csrc.nist.gov/pubs/sp/800/92/final

Used to support the article's distinction between having logs and having managed, preserved, interpretable evidence capable of supporting incident conclusions.

S09 — SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations

Publisher: National Institute of Standards and Technology

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Used to support the article's broader control themes around audit events, access control, accountability, system monitoring, and integrity.

S10 — Digital Evidence Preservation: Considerations for Evidence Handlers

Publisher: National Institute of Standards and Technology

https://www.nist.gov/publications/digital-evidence-preservation-considerations-evidence-handlers

Used to support the article's view that BEC evidence requires preservation discipline, not merely screenshots or workflow exports.

A2 — SOURCE MAPPING

Where the sources apply

The email is not the incident

S01 S02 S04 S05

- Business Email Compromise
- 2024 IC3 Annual Report
- Business payment fraud
- Payment diversion fraud

The real failure is trust conversion

S03 S04 S05 S09

- Business Email Compromise: The $55 Billion Scam
- Business payment fraud
- Payment diversion fraud
- SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations

The missing record is payment authority

S05 S09

- Payment diversion fraud
- SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations

The callback must escape the compromised channel

S04 S05

- Business payment fraud
- Payment diversion fraud

Supplier bank-detail changes are evidence events

S04 S05 S09

- Business payment fraud
- Payment diversion fraud
- SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations

ERP approval is not independent verification

S09 S08 S10

- SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
- SP 800-92: Guide to Computer Security Log Management
- Digital Evidence Preservation: Considerations for Evidence Handlers

BEC exploits hierarchy, not just technology

S01 S05

- Business Email Compromise
- Payment diversion fraud

After payment, timing becomes evidence

S02 S04 S05

- 2024 IC3 Annual Report
- Business payment fraud
- Payment diversion fraud

Insurance, supplier disputes, and recovery all depend on the chain

S06 S07 S04 S05

- 2025 Cyber Claims Report
- Business email compromise tops cyber claims: Coalition
- Business payment fraud
- Payment diversion fraud

The evidence should exist before the attack

S09 S10

- SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations
- Digital Evidence Preservation: Considerations for Evidence Handlers

Public proof does not require exposing payment data

S10

- Digital Evidence Preservation: Considerations for Evidence Handlers

The future of BEC defence is evidence, not awareness

S01 S08 S09

- Business Email Compromise
- SP 800-92: Guide to Computer Security Log Management
- SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations

A3 — SOURCE INDEX

Full source index

S01 — Business Email Compromise

Publisher: Federal Bureau of Investigation

https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/business-email-compromise

Used to ground the article’s treatment of BEC as one of the most financially damaging online crimes and as a fraud exploiting trusted business communication.

S02 — 2024 IC3 Annual Report

Publisher: Federal Bureau of Investigation Internet Crime Complaint Center

https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Used to support the article’s discussion of BEC losses, financial fraud reporting, and the importance of timely reporting to banks, IC3, FBI field offices, and law enforcement.

S03 — Business Email Compromise: The $55 Billion Scam

Publisher: Federal Bureau of Investigation Internet Crime Complaint Center

https://www.ic3.gov/PSA/2024/PSA240911

Used to support the article’s view that BEC has evolved into a global, high-loss fraud category involving exposed losses and increasingly sophisticated techniques.

S04 — Business payment fraud

Publisher: National Cyber Security Centre

https://www.ncsc.gov.uk/section/respond-recover/ml-business-payment-fraud

Used to inform the article’s discussion of fraudulent payment requests, invoice redirection, reporting to IT, contacting the bank directly, and using official contact routes.

S05 — Payment diversion fraud

Publisher: Report Fraud / City of London Police

https://www.reportfraud.police.uk/payment-diversion-fraud/

Used to support the article’s treatment of spoofing, urgency, altered payment instructions, executive or supplier impersonation, secondary verification, multi-person approval, and financial-institution notification.

S06 — 2025 Cyber Claims Report

Publisher: Coalition

https://web.coalitioninc.com/download-2025-cyber-claims-report.html

Used as a market reference for BEC and funds transfer fraud claims activity.

S07 — Business email compromise tops cyber claims: Coalition

Publisher: Business Insurance

https://www.businessinsurance.com/business-email-compromise-tops-cyber-claims-coalition/

Used to support the article’s treatment of BEC as a leading cyber incident type in claims reporting.

S08 — SP 800-92: Guide to Computer Security Log Management

Publisher: National Institute of Standards and Technology

https://csrc.nist.gov/pubs/sp/800/92/final

Used to support the article’s distinction between having logs and having managed, preserved, interpretable evidence capable of supporting incident conclusions.

S09 — SP 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations

Publisher: National Institute of Standards and Technology

https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Used to support the article’s broader control themes around audit events, access control, accountability, system monitoring, and integrity.

S10 — Digital Evidence Preservation: Considerations for Evidence Handlers

Publisher: National Institute of Standards and Technology

https://www.nist.gov/publications/digital-evidence-preservation-considerations-evidence-handlers

Used to support the article’s view that BEC evidence requires preservation discipline, not merely screenshots or workflow exports.

A4 — DOCUMENT CONTROL

Citation and publication history

Suggested citation

EviWrite, "The BEC Evidence Gap: Why Payment Fraud Is Not Just an Email Problem," EviWrite Insights, 2026.

https://eviwrite.com/insights/the-bec-evidence-gap/

Version history

1.0 - 2026-02-21
Initial publication.

1.1 - 2026-05-20
Updated source mappings to match article headings, sharpened payment-authority framing, strengthened proof-before-payment language, and clarified BEC evidence boundaries.

1.2 - 2026-05-25
Reworked article structure, removed repetition, expanded source mappings, added article record, clarified infographic evidential mark, strengthened proof-layer framing, tightened BEC payment-authority analysis, and refined audience-specific implications.

A5 — MACHINE-READABLE INTERPRETATION NOTE

AI summary limits

Business Email Compromise is often treated as an email or phishing incident, but the deeper failure is evidential: the organisation cannot show why a fake instruction became a real supplier change, approval, payment, exception, or bank transfer. The article argues for structured BEC evidence records that connect the instruction, identity, supplier change, verification method, approval, payment release, bank action, insurer notice, recovery attempt, supplier dispute context, and proof boundary.

Interpretation limits

- The article does not provide legal, insurance, banking, cyber-response, fraud-recovery, or jurisdiction-specific advice.
- The article does not claim that every BEC loss is caused by internal control failure.
- The article does not claim that evidence records guarantee payment recovery, insurance cover, liability outcome, regulatory outcome, or prosecution.
- The article does not replace immediate reporting to banks, law enforcement, insurers, or incident-response advisers.

Related pages

Evidencing
Create structured records before payment, supplier, or cyber incident claims are challenged.
https://www.eviwrite.com/evidencing/

Verification
Check bounded claims without exposing sensitive financial, supplier, or security data.
https://www.eviwrite.com/verification/

A6 — GLOSSARY

Defined terms

Business Email Compromise

A cyber-enabled fraud in which criminals use compromised, spoofed, or deceptive communications to cause a business or individual to transfer money, disclose sensitive information, or change payment instructions.

Payment diversion fraud

Fraud in which payment is redirected away from the intended recipient, often through altered bank details, supplier impersonation, executive impersonation, or compromised communications.

Supplier-change evidence

Records showing the source, request, verification, approval, previous state, new state, timing, authority, and proof limits of a supplier or vendor record change.

Independent callback

A verification call or contact made using a trusted source separate from the suspicious request, such as a previously verified supplier record or official contact route.

Payment-authority record

A structured record showing why a payment was allowed, who approved it, what verification occurred, what exceptions applied, and what evidence supported the release of funds.

Proof boundary

The defined limit of what a BEC evidence record proves, what it supports, and what it does not decide.

A7 — QUESTIONS

Common questions

What evidence is needed after Business Email Compromise?

A serious BEC record should preserve the original instruction, sender and account context, supplier or executive impersonation details, verification method, supplier-record changes, approval workflow, payment release, bank transfer, recall attempt, insurer notice, law-enforcement report, and proof boundaries.

Is a fake email enough to prove BEC?

No. The email may prove the attempted deception, but the wider incident record should show how the organisation assessed the instruction, verified identity, approved action, changed records, released funds, and responded after discovery.

Is a callback enough to defend a payment?

Only if the callback is evidenced properly. The record should show the independent contact source, who called, who answered, what was confirmed, what discrepancies existed, and what decision was made from that verification.

Does ERP approval prove the payment was properly authorised?

Not by itself. ERP approval may show that an internal workflow accepted a payment or supplier change, but it may not prove independent verification, genuine supplier authority, or adequate control operation.

What should be done immediately after a fraudulent payment?

At a general level, the organisation should contact its bank through official routes, report internally to cyber and finance teams, preserve evidence, notify relevant fraud-reporting or law-enforcement bodies where appropriate, and notify insurers or advisers according to policy, legal, and incident-response requirements.

Can BEC evidence remain confidential?

Yes. Sensitive financial, supplier, cyber, and legal material can remain private while a bounded proof layer records existence, timing, status, verification actions, and evidence boundaries.