EXECUTIVE RISK BRIEF

THE PAYMENT VERIFICATION GAP

Why large organizations need a human-controlled verification layer before money moves

Prepared for	Chief Financial Officers, Treasurers, Controllers, Accounts Payable, Fraud, Risk, Internal Audit, Procurement, and Compliance Leaders
Prepared by	BSS Technologies Inc. | VYQ OS™ Financial Verification Operating System
Date	July 2026

Money moves when verified.

This brief is intended for executive and operational review. It describes a controlled verification model for high-risk payment decisions, including invoice review, business email compromise, vendor changes, payee validation, and payment approval.

Executive Summary

Large organizations have invested heavily in email security, access controls, approval limits, and fraud detection. Yet a critical gap remains at the moment a payment instruction appears legitimate but the authority, beneficiary, evidence, or change context has not been independently verified.

The FBI describes business email compromise as one of the most financially damaging online crimes. The 2024 IC3 Annual Report recorded 859,532 complaints and $16.6 billion in reported losses, a 33% increase from 2023. Business email compromise alone accounted for 21,442 complaints and approximately $2.77 billion in reported losses.

$16.6B	859,532	$2.77B
Total reported IC3 losses in 2024	IC3 complaints in 2024	Reported BEC losses in 2024

The control problem

A technically authentic email, document, or account can still carry an unauthorized instruction. A valid invoice can be paired with fraudulent remittance information. A familiar executive name can be used to pressure an employee to bypass normal procedure. A genuine vendor relationship can be exploited through a compromised mailbox.

The FBI advises organizations to verify payment and purchase requests through an independent channel and to confirm any change in account number or payment procedure with the person making the request. The missing enterprise capability is often not another alert. It is a repeatable verification gate that converts that advice into a documented operating workflow.

Seven questions before release

- **Authority:** Is the person or system making the request authorized?
- **Business:** Is the organization and relationship legitimate and current?
- **Payee:** Is the intended beneficiary the correct legal and operational recipient?
- **Evidence:** Do the invoice, contract, purchase order, delivery record, and approvals align?
- **Change:** What changed from the established pattern, and why?
- **Confirmation:** Was the request independently verified through a trusted channel?
- **Decision record:** Can the organization reconstruct who approved what, when, why, and with which evidence?

Why Existing Controls Still Leave a Gap

Existing control	What it does well	What can remain unresolved
Email security	Blocks known malicious messages, attachments, and domains.	A compromised legitimate mailbox or authentic-looking thread may still deliver a fraudulent payment instruction.
Multi-factor authentication	Reduces unauthorized account access.	Does not establish that a payment request, beneficiary change, or invoice is commercially valid.
Approval limits	Controls which employees can authorize certain amounts.	An authorized approver can still act on manipulated evidence or false authority.
ERP and AP workflow	Standardizes invoices, purchase orders, and payment processing.	Fraud can enter through vendor-master changes, altered remittance instructions, or weak exception handling.
Bank fraud monitoring	Detects transaction anomalies and suspicious account behavior.	The bank may not have the internal invoice, contract, approval, and vendor context needed to determine business intent.

The verification-gate operating model

A verification gate sits before the final approval or release step. It does not replace the ERP, bank, fraud platform, treasury workstation, or compliance team. It organizes the evidence and decision logic those systems and people need.

Gate	Required proof	Possible status
1. Identity and authority	Known contact, approved role, trusted communication path, valid delegation.	Verified / Watch / Hold
2. Business and payee	Legal entity, vendor record, beneficiary consistency, established relationship.	Verified / Hold
3. Document and transaction	Invoice, purchase order, contract, delivery, amount, timing, rail, and destination.	Verified / Watch / Hold
4. Change and anomaly	New account, changed domain, urgent timing, secrecy, unusual amount, duplicate request.	Watch / Hold / Reject
5. Independent confirmation	Callback or confirmation using a previously trusted source, not information in the request.	Verified / Hold
6. Human approval and audit	Named reviewer, reason codes, evidence references, timestamp, escalation, final authority.	Proceed / Escalate / Do not proceed

VYQ OS: Governed Verification Before Money Moves

VYQ OS is a human-controlled Financial Verification Operating System developed by BSS Technologies Inc. It is designed to support evidence-based review of invoices, business email compromise concerns, vendor changes, payee reviews, and payment approvals.

The system's purpose is not to make an uncontrolled autonomous payment decision. Its purpose is to structure the verification process, preserve human authority, explain why a case was approved or held, and maintain a reviewable decision record.

Core capabilities

Capability	Enterprise value
Structured intake	Captures the business-safe facts, claimed authority, payment context, change details, and requested outcome.
Evidence organization	Records invoice, contract, purchase order, identity, vendor, payee, and confirmation evidence or references.
Risk-signal review	Flags urgency, changed instructions, inconsistent domains, new beneficiaries, missing evidence, and policy exceptions.
Decision status	Supports clear statuses such as Verified, Watch, Hold, or Reject / Do Not Proceed.
Reason codes and explanation	Documents the conditions that produced the status and the evidence needed to resolve a hold.
Human approval	Preserves reviewer authority and escalation rather than allowing AI to release money.
Audit trail	Maintains a timestamped record of submission, review, evidence, status changes, recommendation, and final disposition.

Controlled operating boundary

VYQ OS is not a bank, payment rail, payment processor, money transmitter, custodian, escrow service, lender, law firm, law-enforcement agency, emergency service, financial advisor, or replacement for an organization's compliance obligations. It does not require customers to submit banking passwords, MFA codes, full account numbers, card numbers, CVV, private keys, or full Social Security numbers.

Human control is the point

AI assistance may help organize information, identify inconsistencies, and prepare explanations. The named organization and authorized reviewers retain final authority. No payment is released simply because an automated score appears favorable.

How an Enterprise Can Evaluate the Model

Evaluation stage	Scope	Evidence produced
Focused executive review	One high-risk payment, vendor-change, invoice, or approval workflow.	Written decision brief, risk signals, evidence gaps, and recommended next action.
Controlled institution access	Defined team, workflow, use cases, users, status rules, and monthly review.	Case records, decision outcomes, audit samples, cycle-time and evidence-completeness measures.
Enterprise implementation	Custom architecture, governance, integration, security, procurement, legal, and operating terms.	Approved implementation plan, control design, training, SOP, and enterprise reporting model.

What corporate leaders should measure

A verification program should be judged by operational outcomes, not by the number of AI features deployed.

Measure	Management question
Payment-loss exposure reviewed	What dollar value of high-risk payments or changes passed through the verification gate?
Potential loss avoided	What amount was held or redirected because material inconsistencies were identified?
Verification cycle time	How long did it take to move from intake to a documented decision?
Evidence completeness	What percentage of cases contained the required invoice, authority, payee, confirmation, and approval evidence?
Change-confirmation rate	Were vendor, beneficiary, and payment-procedure changes independently confirmed?
Hold-resolution rate	How many held cases were resolved with sufficient evidence versus rejected or abandoned?
Audit reconstruction	Can internal audit reconstruct the decision without relying on employee memory or scattered email?

Executive Conclusion

Large organizations do not need another system that simply produces more alerts. They need a governed process that can answer a more important question:

> **Is this particular payment decision supported by verified authority, verified business context, verified payee information, sufficient evidence, independent confirmation, and an accountable human approval?**

The next stage of financial AI should not be uncontrolled autonomy. It should be governed verification.

Recommended next step

Begin with a controlled executive review of one high-risk payment, vendor-change, invoice, payee, or approval workflow. The objective is not to replace the current control environment. It is to determine whether a verification gate can improve evidence completeness, decision traceability, and risk handling before money moves.

Review the VYQ OS approach https://www.bsstechnologiesinc.com/VYQ.html	**Focused Payment Risk Review** https://www.bsstechnologiesinc.com/VYQ/vyq-payment-risk-review.php
Executive contact Lathell Sancho, Founder and CEO l.sancho@bsstechnologiesinc.com	**General contact** info@bsstechnologiesinc.com BSS Technologies Inc.

Sources

1. Federal Bureau of Investigation, Internet Crime Complaint Center, *2024 IC3 Annual Report*, pages 3-10. The report states that IC3 received 859,532 complaints in 2024, with $16.6 billion in reported losses; Business Email Compromise accounted for 21,442 complaints and $2,770,151,146 in reported losses.

2. Federal Bureau of Investigation, *Business Email Compromise*. The FBI advises organizations to independently verify payment and purchase requests and confirm any change in account number or payment procedure with the person making the request.

Source access date: July 14, 2026. Statistics reflect reported complaints and losses and should not be interpreted as the total incidence or total economic impact of fraud.

BSS Technologies Inc.
VYQ OS™ Financial Verification Operating System
Money moves when verified.