An nsKnox guide

When Fraud Comes From Within: A Deep Dive Into Insider Threats in Corporate Payments

Why does only a technology-driven approach work and the 5 pillars of tamper-proof protection

nsknox

nsknox

CONTENTS

The rising toll of insider-driven payment fraud

Business-to-business (B2B) payment fraud is more pervasive and damaging than ever.

The number of annual attacks and the scope of losses continue to rise, placing organizations under unprecedented pressure to safeguard their financial operations.

Among the most pressing threats to B2B payment fraud is that posed by insiders.

B2B payment fraud is everywhere

79%
of companies were hit in 2024

>$100
million can be lost in a single incident

45%
of businesses have faced a breach tied to payment fraud

Beware of insiders

57%
of fraud is committed by company insiders

31%
of the most disruptive fraud is internal

$15M
is the average cost of an insider incident

Prevention is more challenging than ever

The high rates of attack and increasing extent of damage should come as no surprise when considering how challenging protection is.

In fact, securing B2B payments against insider fraud has become one of the most complex challenges that finance teams face today, as insiders are often aware of the weak points in systems and controls.

The attack surface is growing

As companies adopt faster payment systems and expand global transactions, the attack surface continues to grow, creating more opportunities for fraud to slip through.

Every type of payment is targeted

Insiders, whether acting alone or manipulated by external actors, don't limit themselves to one side of the transaction. They exploit their access to divert outgoing payments and manipulate incoming ones.

On the outgoing side, they infiltrate payment processes to reroute company funds, using tactics like Business Email Compromise (BEC), email account takeover, and others to make fraudulent payments look entirely legitimate.

The result can be severe consequences, including:

And indeed, the challenges are formidable:

- The **attack surface** is growing
- **Every type** of payment is targeted
- Perpetrators exploit **powerful new technologies**

> "Although organizations remain vigilant in combatting payments fraud, many continue to be victims of fraud, as scammers have become more sophisticated with the help of AI and other technologies."
>
> 
>
> **Jim Kaitz,**
> President & CEO of AFP

- Substantial financial **losses**
- Operational **disruptions**
- Reputational **damage**

On the incoming side, the scheme plays out differently, but with the same devastating result, where criminals tamper with invoices or alter banking details, causing customers to unknowingly send payments to fraudulent accounts.

Instead of reaching the organization's bank, revenues are quietly redirected elsewhere, eroding both cash flow and customer trust.

Perpetrators exploit powerful new technologies

Social engineering schemes today exploit sophisticated new technologies such as deepfake AI, enabling fraudsters to impersonate trusted parties and trick employees into approving fraudulent payments (read more in our blog).

And advanced cyberattacks, from credential theft to direct ERP intrusions, can be launched to compromise systems and infiltrate payment workflows.

When insiders deploy these strategies and tactics, or when external fraudsters recruit or trick them to do so, the repercussions are severe. This is because they are all too familiar with an organization's vulnerabilities, enabling them to bypass controls, manipulate documents and master data, forge invoices and account details, and cover their tracks with alarming ease.

According to the 2024 Fraud Insights Report, the need for advanced fraud prevention strategies to address the challenges posed by insider threats within organizations has never been greater.

Why traditional defenses fall short

Organizations have long relied on a patchwork of manual checks and basic controls to guard against B2B payment fraud, whether perpetrated by insiders or external actors.

These measures may have worked to some degree in the past, but they are error-prone, difficult to scale, and no match for today's sophisticated fraud tactics.

Common manual defenses (and their pitfalls)

Email-based invoice approvals	Invoices are routed to department heads for sign-off, but approvals can be easily forged and challenging to track during audits.
Manual invoice-to-PO matching	Manual checks slow operations, are vulnerable to errors, and often break down as invoice volumes rise.
Check runs with CFO signatures	Intended to centralize oversight, they create bottlenecks and single points of failure.
Callbacks and W-9 forms	Used to verify vendor details, they can be easily manipulated or forged by determined fraudsters.
Dual approvals	Splitting responsibility across two approvers often devolves into rubber-stamping when workloads are high.

When insiders target payments: real-world cases

Behind the statistics are real stories of insiders and manipulated employees misappropriating millions from organizations that trusted them.

These cases illustrate how fraud can hide in plain sight, bypassing controls for months and even years, before the damage is revealed.

Bridgestone:

The $15M fake vendor scheme

A senior treasury official at tire manufacturer Bridgestone created a fictitious vendor and funneled $15 million through fraudulent invoices over the course of four years. His position allowed him to approve payments without question, exposing how easily trust and manual processes can be abused.

Dixon, Illinois:

A $54M deception

For over 22 years, a town comptroller in Dixon, Illinois, embezzled $54 million, exploiting her insider access to falsify records and divert funds. The scheme went undetected for decades, crippling local finances and highlighting how long insider fraud can persist.

Macy's:

$130M hidden in the books

In an effort to mask a bookkeeping mistake, a single employee at the retail giant concealed over $130 million in delivery expenses by manipulating accrual entries across several quarters. The fraud delayed earnings announcements and impacted share value.

ConocoPhillips:

$3.2M in contracts for nothing

Two conspirators, including one ConocoPhillips employee, used a fabricated vendor to bill for non-existent goods and services, extracting $3.2 million from the energy corporation. With inside authority and forged records, they created a paper trail of lies, which investigators eventually exposed as fraudulent.

Orion:

The $60M BEC case

An Orion employee was tricked into wiring $60 million overseas by cybercriminals impersonating trusted partners. The BEC attack compelled the company to record a one-time, pre-tax charge of $60 million and engage in legal battles to recover the funds.

The bottom line

What makes insider-driven fraud so dangerous is not just access, but trust. Insiders are often granted authority that allows them to override safeguards, making their schemes both harder to detect and far more costly when discovered.

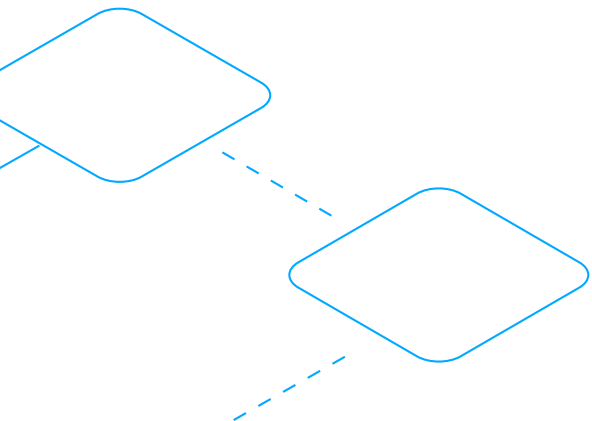
The problem is compounded by outdated defenses. Traditional models assume trust within the organization and rely on manual validation processes that fraudsters can easily bypass. Relying on outdated approaches is no longer an option. The risks are simply too high.

The path forward is clear. First, organizations must adopt a zero-trust mindset where no transaction, user, or system is accepted at face value.

And – the only way to mitigate risk is through a technology-driven approach that ensures payments are made to valid accounts only, as driven by the five pillars of robust, end-to-end protection, i.e.:

- Verifying both **incoming and outgoing** payments
- Validating **any account anywhere** in the world
- Ensuring **master data security**
- Offering **flexibility** for both instant searches and extensive, vendor-verified checks
- **Automatically scanning** master data and every payment transaction for immediately flagging anomalies

Only by moving beyond manual processes with automated, technology-based, and highly secure protection within the payment flow can organizations truly safeguard their assets, protect stakeholders, and preserve their financial health.



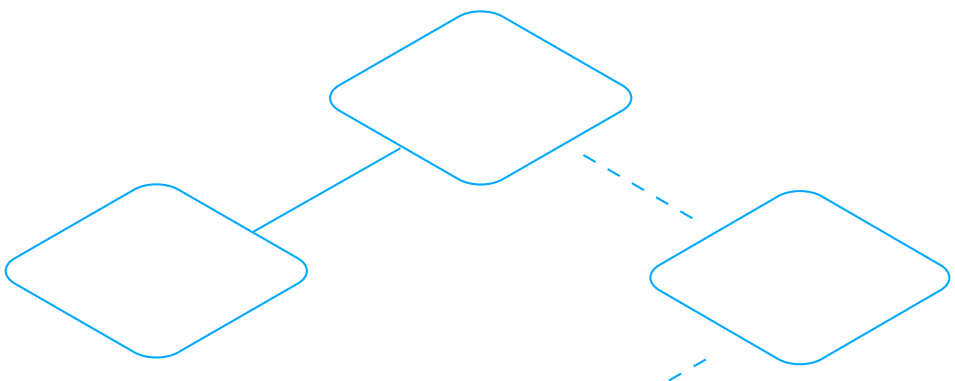
How nsKnox can help

With PaymentKnox™, nsKnox delivers what today's organizations need – an **automated, technology-driven, and tamper-proof solution** that protects both outgoing and incoming B2B payments from insider fraud, manipulation, and abuse.

The end-to-end platform eliminates the vulnerabilities of manual processes with full coverage across the five pillars of robust protection:

- **Validating any account, anywhere in the world** – with Adaptive Payment Security™ for both rapid, low-effort validations when speed is critical, as well as in-depth, out-of-network verification when risk is high, for ultimate certainty.
- **Offering flexible verification options** – from rapid in-network searches with Quick Check™, as well as robust, vendor-verified, out-of-network validations with Knox Verify™, for high-risk cases.
- **Securing master data** – with Master Data Guard, which protects the vendor file from tampering and maintains integrity over time.
- **Automatically scanning every payment and master data record** – with Payment Check, which continuously audits transactions and flags discrepancies or exceptions.

And, for ensuring **tamperproof security**, nsKnox's patented Cooperative Cyber Security™ (CCS) technology makes manipulation virtually impossible by mathematically shredding and distributing sensitive data across multiple independent entities.

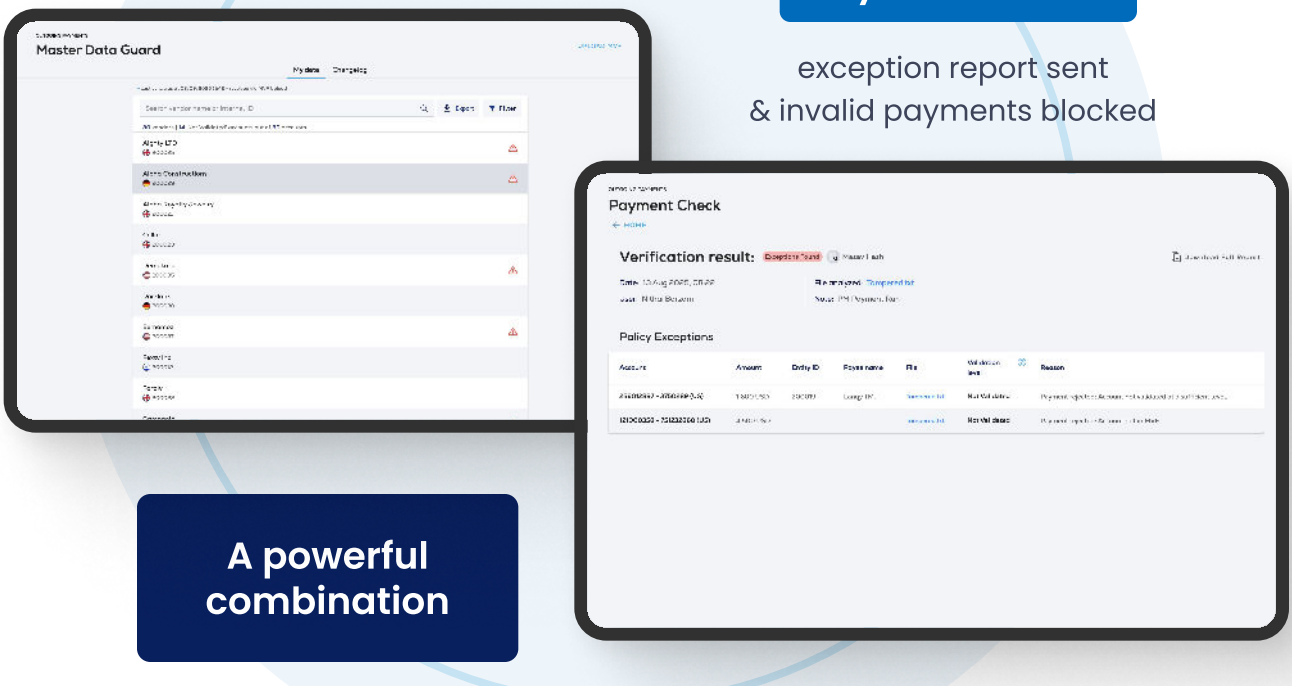


Master Data Guard

supplier, account, or new information is identified as not yet validated

Payment Check

exception report sent & invalid payments blocked



A powerful combination

With this combination of technologies, solutions, and protections, nsKnox enables organizations to:

- **Safeguard** the company, its vendors, and customers from the most elusive types of fraud
- **Detect** manipulation instantly with automated alerts on discrepancies
- **Eliminate** the costly errors of manual processes
- **Protect** both accounts payable and receivable against fraud that threatens cash flow
- **Accelerate** time to value with seamless integration, minimal IT effort, and zero changes to existing workflows

Treasurers, controllers, and risk managers agree

"Knowing that every single employee in Treasury is using the same centralized process, and the fact that we have mitigated any fraud or human error risk gives me peace of mind that our Treasury operations can continue to run smoothly."

Cathy Cantasano
CTP. Executive Director, Treasurer
W.P. Carey Inc.

Read the story →

"At BabcockPower's finance team, we recognized the critical importance of protecting our payments and proactively sought a robust, technology-based solution that will eliminate the need to rely on manual processes, which are error-prone. Our search quickly led us to nsKnox, whose automated, deterministic validation process has been instrumental in safeguarding our financial operations."

Laura S. Gouzie, CTP
VP Treasury & Insurance Risk Management
BabcockPower

Read the story →

"nsKnox plays a vital role in our best practices. Before releasing payment files to our bank, we leverage the nsKnox portal to scan the payment instructions, ensuring they match what's in the database. Any discrepancies are highlighted, allowing us to correct the instructions or investigate potential fraud before the bank releases the payment."

Peter Rudzinski
Director of Risk Management
Brunswick

Read the story →

"We saw results from nsKnox very quickly. We were able, for the first time, to validate accounts in any country we operate in, and we realized that the continuous validation of the accounts in the ERP system is important for keeping the integrity of the accounts' details. The decision to launch the technology in all sites was a natural next step for us."

Robert (Bob) Bonacci
Corporate Controller
Ansys

Read the story →

In conclusion

Insider-driven payment fraud is one of the most dangerous financial threats organizations face, because those with access know precisely how to slip past defenses.

Manual checks and outdated controls no longer stand a chance against the latest and greatest in the fraudster's toolkit.

Only a technology-driven shield can close the gap. And that's what nsKnox brings – tamper-proof, automated, technology-based global protection that makes even the most sophisticated insider schemes impossible to succeed.

About nsKnox

nsKnox is a fintech-security company, enabling corporations and banks to prevent fraud and ensure compliance in B2B Payments. Leveraging its patented Cooperative Cyber Security™ (CCS) and groundbreaking Bank Account Certificate™ technology, nsKnox's solutions detect and prevent finance and ops infrastructure attacks, social engineering, business email compromise (BEC), insider fraud, and other Advanced Persistent Fraud attacks. For more information, go to www.nsknox.net