

PaymentKnox

Prevent Corporate Payments Fraud

Cybercriminals today are increasingly targeting corporate payments in their efforts to defraud organizations out of millions of dollars.

 82%

of organizations fall victim to payments fraud

 5%

of revenues are lost to fraud annually

 <25%

of losses are recovered by most victim companies

With the escalation of annual attacks and financial damages, it is clear that existing controls and security measures are simply not robust enough.

As such, these processes remain extremely vulnerable to cyberfraud attacks, social engineering and insider fraud.

What's needed is a new way to protect corporate payments, by:

- Enhancing how payee details and change requests are verified, with current means being highly prone to error, and vulnerable to social engineering.
- Ensuring that payments are verified at every stage of processing.
- Automating payments-related processes and security checks, to avoid errors and security vulnerabilities.

Protect Your Payments

The PaymentKnox solution enables organizations to minimize the risk of human error and prevent unauthorized payments by detecting and preventing social engineering attempts, insider fraud, and multiple other types of cyberfraud attacks.


nsknox

A Global Payee Directory

contains the details of payees from around the world, enabling organizations to seamlessly and easily validate, and continually verify payee details before making payments, thus avoid the damage of social engineering attempts to intercept payments.

Account Validation

is a set of services for validating payee bank account details during onboarding or when making changes to the bank account on record. This highly secured, yet quick and easy process overcomes the weaknesses of today's means for validating account details, which are commonly and easily exploited by cybercriminals. As a result, organizations gain the confidence that payee details are verified and that the relevant bank account information is validated.

Real-Time Payment Check

detects, alerts and prevents cyberfraud attempts in real time. It verifies every destination account before payments are transferred, generates alerts to changes made to the Master Vendor File (MVF) and blocks payments that are detected as on route to unauthorized accounts. The real time and active protection ensures that every payment is transferred only to the intended payee and account, every time, keeping fraudsters at bay with supremely robust cyberprotection.

Cooperative Cyber Security™ (CCS)

ensures that all payee and payment related data can't be accessed by unauthorized users. It is a unique, tamper-proof platform that was developed by nsKnox, and which underlies all our solutions. Protection is ensured by digitally shredding data, encrypting each separate piece, and storing these pieces across multiple, distributed, highly-secured networks. Through this approach and by leveraging nsKnox's powerful cybersecurity technology, CCS ensures that payee and payments-related data is inaccessible to fraudsters.

Game-Changing Capabilities



On-Going Verification

via a global directory where payee data is registered and continually verified



Payee Account Validation

with a digital process that bypasses the most frequently exploited vulnerabilities



Real-Time Protection

by detecting, alerting, and preventing cyberfraud attempts before they happen



Tamper-Proof Security

with a unique framework for exponentially stronger data protection through multiple, distributed, highly-secured servers

To get started today we invite you to reach out to us at contact@nsknox.net.