trustmi

BEHAVIORAL AI FOR PAYMENT SECURITY

Modern Fraud Arrives “Pre-Approved”

AI has expanded the scale, realism, and complexity of B2B payment fraud.

Trustmi has visibility into more than **$240 billion in enterprise B2B payments**. Using that dataset, we analyzed **260 real-world payment fraud attacks** to understand how they are built.

Payment Fraud Isn’t Breaking Controls. It’s Passing Them.

Fraud now has everything it needs to move from first touch to final payment: a way in, a trusted name, room to move through your systems, convincing documentation, and a clean bank account.

Finding The Entry Point

85% of attacks began in email and went undetected

Access gained through a trusted email conversation

Building Authority

92% of attacks impersonated vendors or executives

A trusted identity was impersonated to authorize the request

Creating Legitimacy

39% of attacks used fraudulent financial artifacts

Financial documents were used to support a payment request

Wiring The Money

90%+ of fraudster bank accounts were legitimate

Funds directed to an attacker-controlled bank account

The Tactics Behind Modern Payment Fraud

Modern payment fraud relies on tactics that follow legitimate vendor processes, using identity, documentation, and workflows to appear routine and pass controls like bank validation.

When Fraud Becomes Layered

Modern payment fraud rarely relies on just one trick.

59% of incidents used two or more coordinated tactics.

- Look-alike domains
- BEC & VEC
- Fake financial documents

When Context Creates Credibility

Fraudsters manipulate requests to appear part of routine business processes.

4 out of 10 fraudsters used communication and contextual tactics.

- Look-alike domains
- Prior comms impersonation
- Fabricated email threads

When Payables Become the Attack

Fraudsters use financial documents to make payment requests appear legitimate.

39% used fraudulent financial artifacts.

- Fake invoices
- Fake W-9 forms
- Fake bank documents

When Banks Say It’s Legitimate

Banks validate fraudster-owned accounts and approve accounts under real vendor names.

90% of accounts were located in the same area as the impersonated vendor.

- Active bank accounts
- Same region as vendor
- In good standing

Reuseable Playbooks Dominate Modern Fraud

The research identifies three primary fraud playbooks:

41% of attacks

The Simple Playbook – reflects the traditional fraud model most organizations already recognize.

Common signals:

- Look-alike domains
- Compromised business email accounts
- Executive impersonation

35% of attacks

The Layered Invoice Playbook – introduces documentation to reinforce legitimacy.

Common combinations:

- Invoice + fabricated email
- Invoice + similar domain
- Invoice + BEC

24% of attacks

The Administrative Playbook – mimics routine vendor validation processes, introducing documentation.

Common patterns:

- Invoice + W-9 + fabricated email thread
- Invoice + W-9 + fabricated email thread + bank document
- Invoice + bank document + similar domain

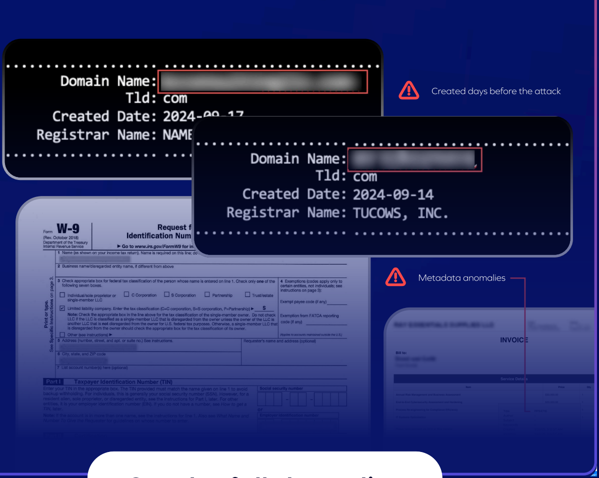
Deep Dive 1

Executive Impersonation

Time Period: **Sep 2023–2025**

Funds Exposed: **~$1M**

A $60K monthly invoice became a $1M fraud—through AI and persistence.



Get the full deep dive

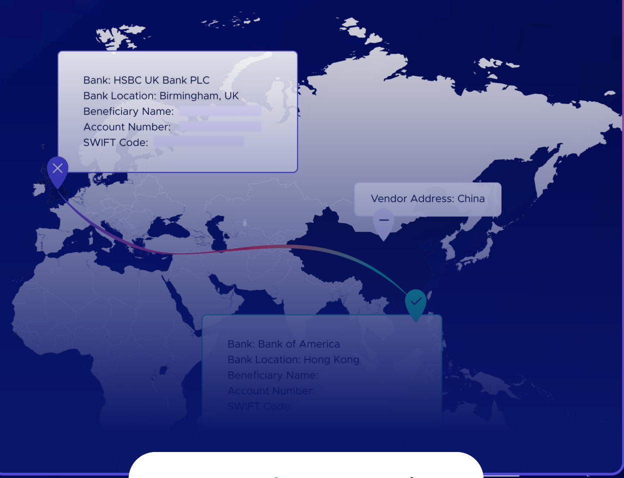
Deep Dive 2

Vendor Impersonation

Time Period: **Sep 2025**

Funds Exposed: **Not disclosed**

A single email thread. A fake vendor. A redirected payment.



Get the full deep dive

B2B Payment Fraud Is Becoming a Workflow Risk

For CFOs and CISOs, the implication is clear: payment fraud is no longer just a communication problem. It is a workflow problem, designed to pass through security and financial controls. Organizations must move beyond siloed defenses and secure the payment workflow end to end.

Read the complete Trustmi Payment Security & Risk Report 2026 here, and join Trustmi Co-founder and CTO, Eli Ben Nun for a live webinar on April 14, 2026 discussing these findings.

Visit trustmi.ai