trustmi

The Trustmi 2025 Socially Engineered Fraud & Risk Report

How Misalignment Between Finance and Security Fuels Financial Loss in the GenAI Era

Table of Contents

Executive Summary

Socially engineered fraud is thriving not only because it's supercharged by GenAI, but because enterprise defenses remain fragmented, split by silos in visibility, ownership, and controls.

In the past year, *The Trustmi 2025 Socially Engineered Fraud & Risk Report* found that **83.6% of enterprises** were targeted by fraud at least once. The survey, based on 525 finance and security professionals at U.S. enterprises with $1B+ in revenue, showed **nearly half** suffered a direct financial loss. Of those, **more than half lost over $500,000** in a single incident.

83.6%
of Respondents
Reported at least one fraud attempt in the last year

It's not just that GenAI is exponentially scaling the number of attacks that lead to these significant losses. Misalignment between teams, systems, and controls was one of the most common drivers of fraud.

One-third of respondents (34.5%) cited finance–security misalignment as a factor in a recent fraud or near miss. When teams are not in sync, gaps in ownership, visibility, and response become exploitable entry points.

35%
of Respondents
Cited finance–security misalignment as a factor in a recent fraud or near miss

The scale of the attack surface compounds the risk. **More than 70% of incidents** spanned multiple systems, bypassing tools and processes of several teams. Legacy safeguards like training, bank validation, and email security were among the most common failures.

In the GenAI era, silos are no longer inefficient; they are an exploitable weakness. As attacks grow in speed and complexity, the gap between fragmented defenses and coordinated fraud will only widen unless enterprises unify visibility, ownership, and response.

About the Survey /

This report is based on Trustmi's Q2 2025 survey of **525 mid-to-senior finance and cybersecurity professionals from U.S. enterprises with $1B+ in annual revenue.**

Industries Surveyed

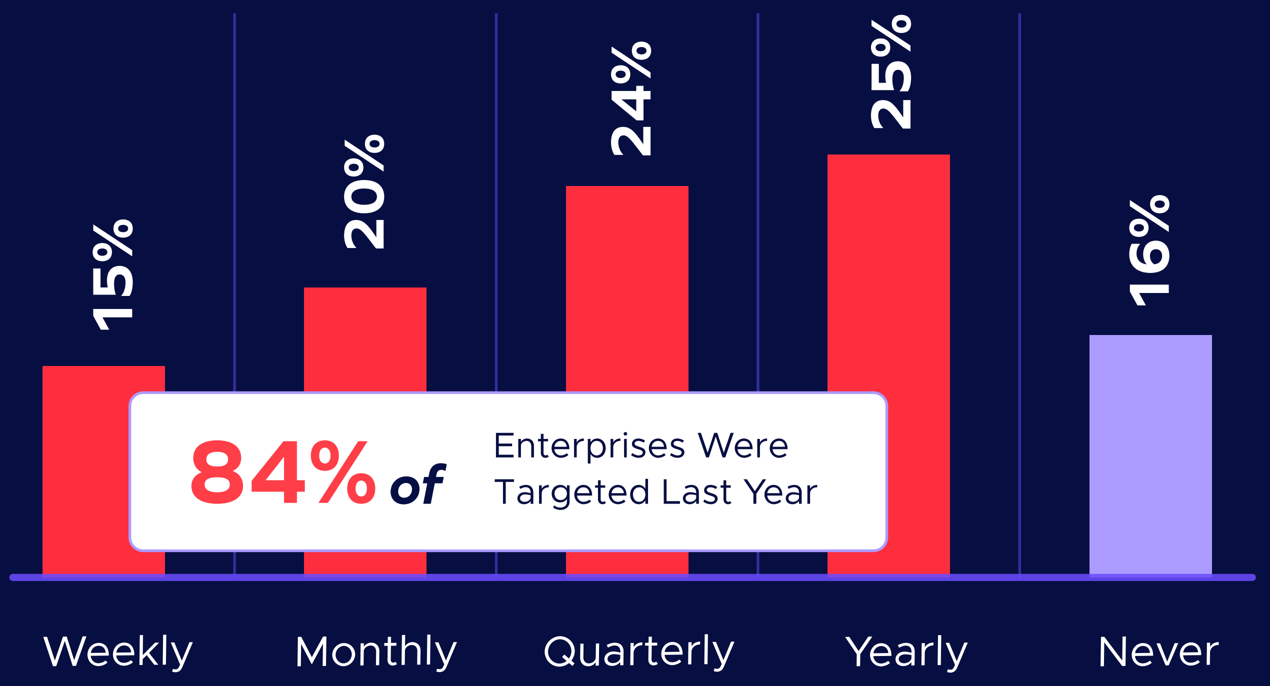
Financial Services
Technology
Healthcare
Manufacturing
Retail

Focus Areas

- Prevalence and cost of socially engineered fraud.
- Alignment between finance and security teams.
- Effectiveness of existing fraud controls.

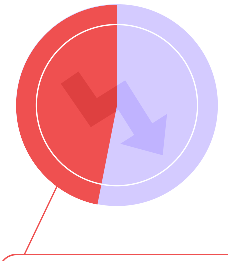
At a Glance

1 *Fraud Is Persistent, Not Rare /*



84% of Enterprises Were Targeted Last Year

2 *Losses are Too Big To Treat as Incidental /*



47.6% Reported a Direct Financial Loss

Over half of those losses were **$500K+** in a single incident.

3 *Modern Attacks Exploit Silos /*

70% of Incidents Crossed Multiple Platforms

Email **ERP** **Vendor Systems** **Payments**

Fewer than **3 in 10** always know about incidents in the other department.

4 *Silos Between Finance and Security Create Blind Spots /*

Only **27%** Say Fraud Prevention Is a Shared Responsibility Between Finance and Security

1 *in 3* Incidents Tied to Poor Coordination

5 *The Old Fraud Playbook Can't Keep Up /*

9/10 Companies Saw at Least One Fraud Control Fail In a Major Incident

Trusted safeguards were the most likely to fail.

Email Security **Manual Verification** **Training**

Everyday Fraud, Extraordinary Costs

Socially engineered fraud isn't rare—it's routine. Nearly a quarter of survey respondents said they're targeted multiple times a year, and 15.7% reported attacks weekly or more. Generative AI has only lowered the barrier for attackers to run more frequent, convincing campaigns.

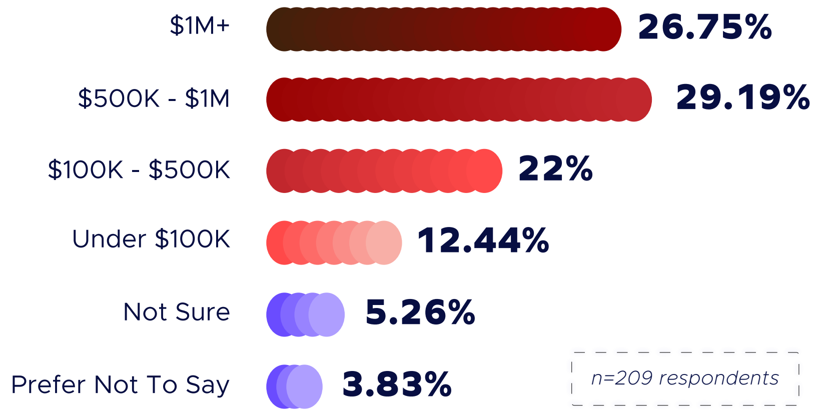
Nearly 1/6
Companies Faces Fraud Attempts Every Week

When these attacks succeed, the cost is steep. Nearly half of the companies surveyed (47.6%) reported a direct financial loss. Among those, the damage was significant: over half lost $500K+ in a single incident.

But fraud doesn't just drain the balance sheet. It ripples across the business. When asked about the most significant incident they experienced, respondents revealed a much broader impact.

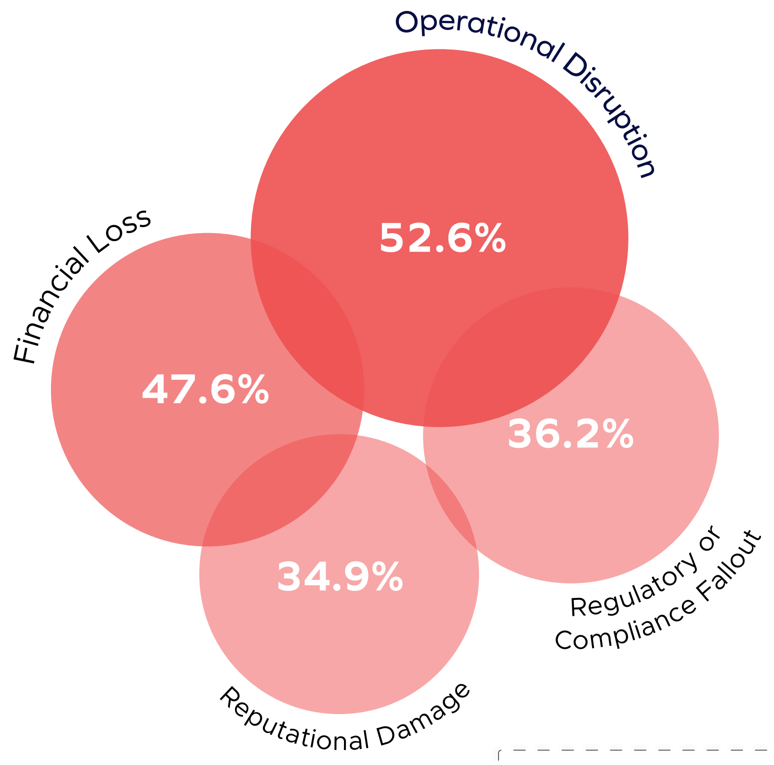
Fraud Losses in a Single Incident /

(Among companies that reported a direct loss)



n=209 respondents

Impact of the Most Significant Incident /



Multiple responses allowed.

Fraud halts processes. It triggers audits and regulatory scrutiny. It damages internal trust and often pulls in legal, IT, finance, procurement, and the C-suite.

Why It Matters /

Fraud is often treated as an acceptable cost of doing business—an occasional loss, tallied and absorbed. But the data shows otherwise. These attacks are frequent, costly, and disruptive. This is not incidental risk; it is cumulative, operationally significant, and growing.

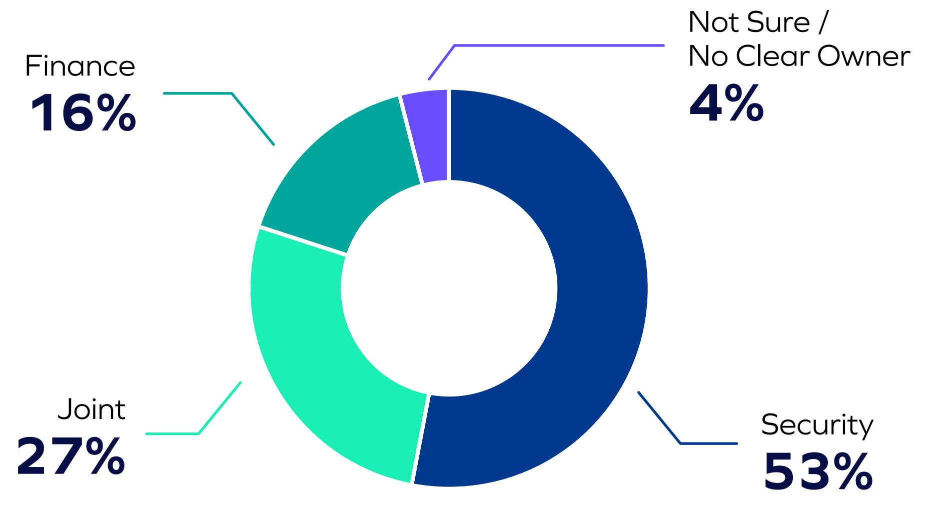
Generative AI accelerates the risk, enabling faster, more personalized, and more coordinated campaigns. But the problem isn't just the scalability of GenAI. It's about where bad actors strike. Today, socially engineered fraud thrives in the gaps between teams and processes, exploiting misalignment in ways traditional controls can't see.

Collaboration Gap Between Finance and Security

The steep financial losses enterprises reported don't come from frequency alone. They reflect where attacks land: in the gaps between finance and security. Unclear ownership leaves openings, and each handoff creates risk that fraudsters exploit.

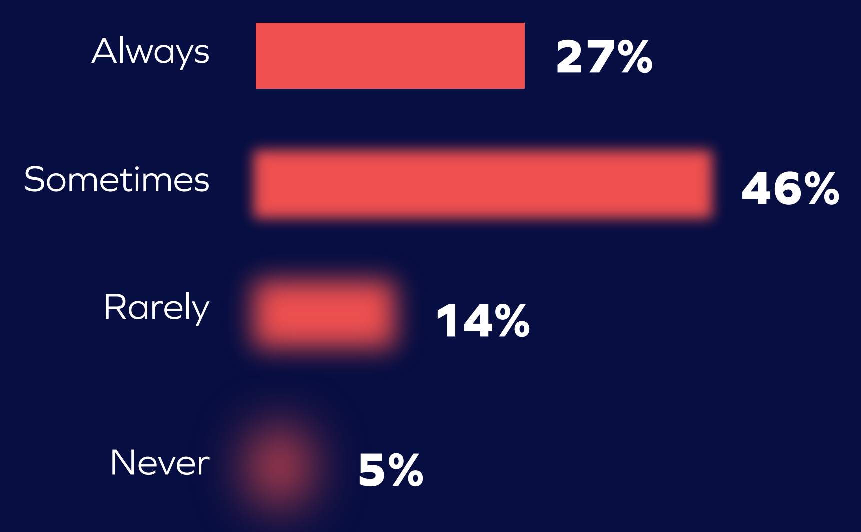
At first glance, collaboration appears solid: 54.3% describe their cross-functional collaboration as "strong," and another 36.2% say it's "moderate." On paper, that suggests alignment. In practice, ownership tells a different story.

Who Owns Fraud Prevention /



A third of organizations (34.4%) reported that gaps in collaboration were a factor in a recent fraud incident or near miss. That divide has real consequences.

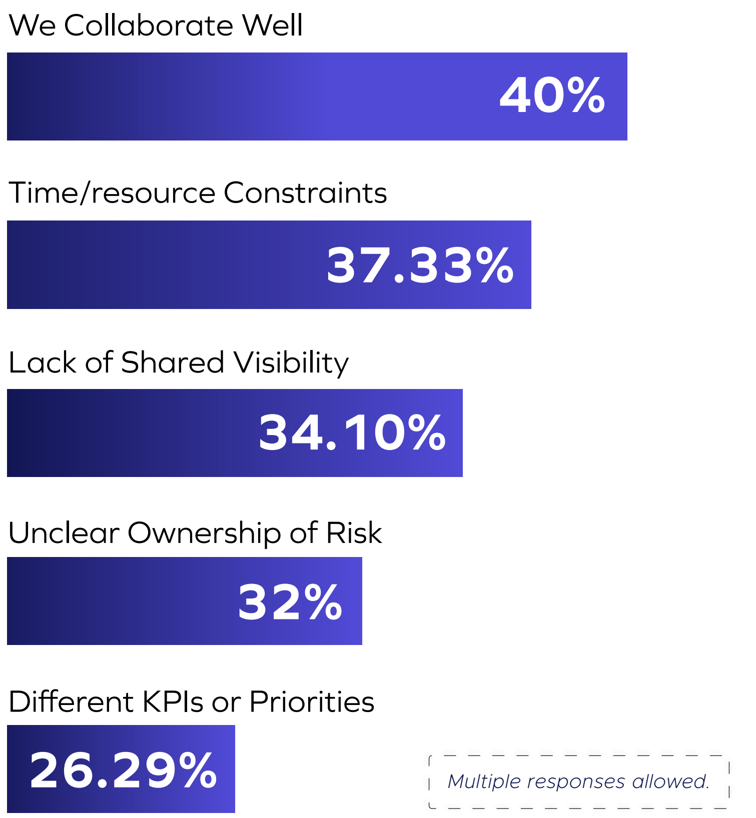
Visibility Into Each Other's Incidents /



Even with integrated tools, visibility remains thin—only 27% say they always know when the other team has discovered or handled a fraud case. Just over a quarter say they always know when the other team has discovered or handled a fraud case.

When asked what most often slows down collaboration, many respondents pointed to structural and operational barriers, including unclear ownership, siloed visibility, and misaligned KPIs.

Top Barriers to Collaboration /



Multiple responses allowed.

Why It Matters /

Collaboration breaks down less from intent and more from structure: without shared visibility, clear ownership, and coordinated responses, gaps remain exploitable.

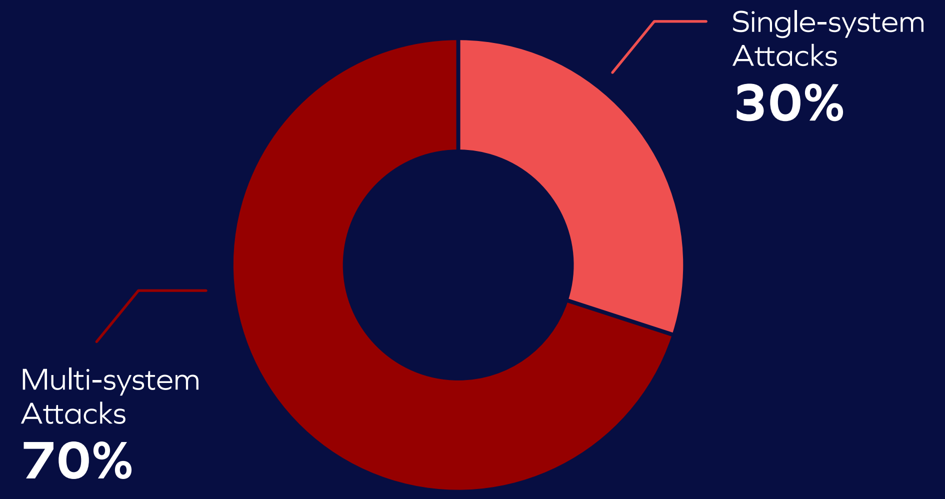
Companies don't need more meetings; they need connected context. Until finance and cybersecurity operate with a unified view of risk, socially engineered fraud will continue to exploit the gaps between systems, signals, and teams and hit the bottom line.

Social Engineering's Attack Evolution

The gaps between finance and security aren't the only problem. Those gaps also define the attack vectors themselves. When an incident moves from email to ERP, or from a vendor portal to a payment system, it's also moving between teams. And every one of those handoffs is a chance for attackers to hide in plain sight.

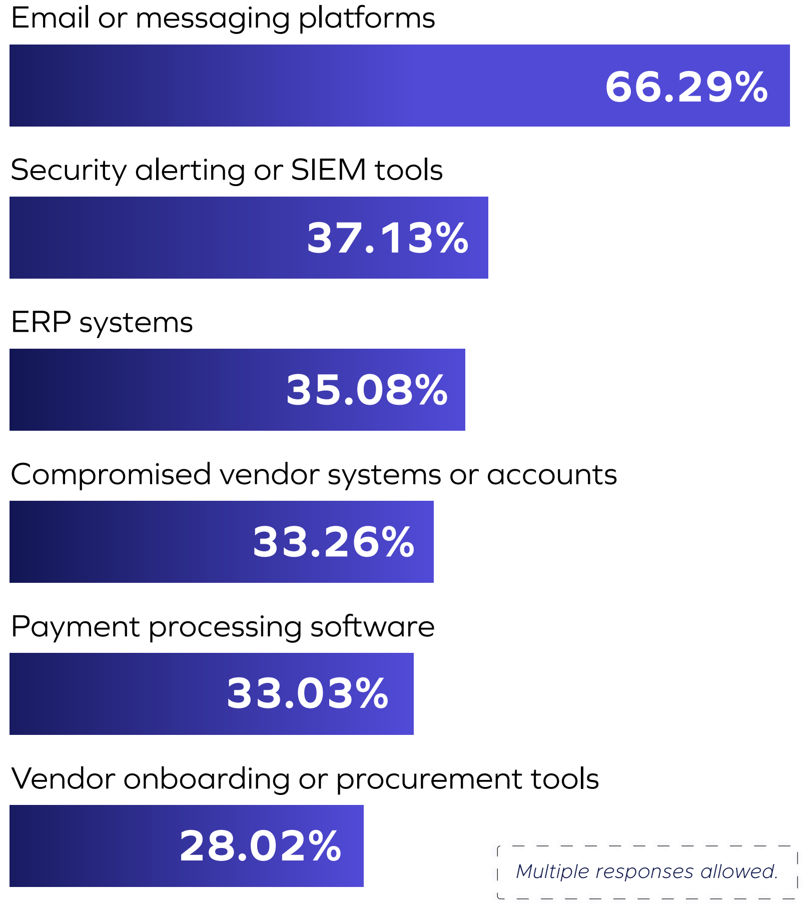
In our survey, 70% of respondents said recent attacks touched multiple systems—from email and ERP platforms to vendor portals and payment software.

Multi-System vs. Single-System Attacks /



These multi-system attacks aren't random. They're designed to bypass controls and stay hidden. Our data indicates that multi-system attacks often coincided with control failures. And with GenAI, they can now automate much of that sequencing.

Systems Involved In Recent Attacks /



Multiple responses allowed.

But systems are just the canvas. The tactics themselves are multiplying. Respondents reported a broad mix of methods that are often used in sequence to compromise workflows and impersonate trust.

Attack Types /

48%	Invoice Fraud	40%	Compromised Third Party
48.5%	Spoofed Login	37%	Insider Fraud
42%	Vendor Impersonation	35%	Deepfake or Synthetic Attack
41.5%	Business Email Compromise		

Multiple responses allowed.

A spoofed login may precede vendor impersonation. A compromised third party may set the stage for a fraudulent invoice. This is full-spectrum deception designed to exploit operational complexity.

Why It Matters /

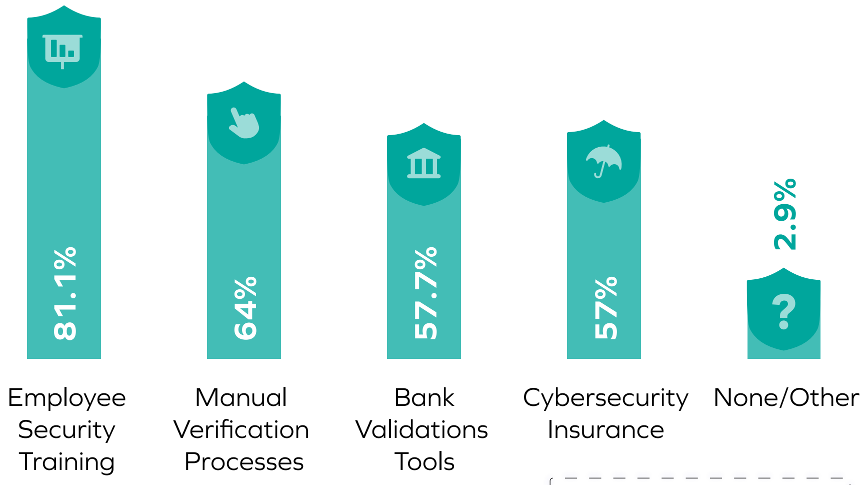
Most enterprise defenses are still single-system tools: email gateways for phishing, ERP rules for approvals, SIEMs for security alerts. But modern fraud doesn't stay in one lane. It flows across systems, blending into normal workflows, and each system has its own blind spots.

When finance, procurement, and security each see only their part of the sequence, no one connects the pattern. That's how sophisticated fraud succeeds: not by breaching a single firewall, but by slipping through the handoffs between systems, signals, and teams.

Traditional Safeguards Are Falling Short

The picture that emerges is clear: today's fraud isn't contained by system boundaries, yet most defenses are. Tools built for a single environment can't follow an attack as it moves from email to ERP to vendor platforms to payment systems. Each handoff is a blind spot, and the more complex the sequence, the easier it is for fraud to slip through.

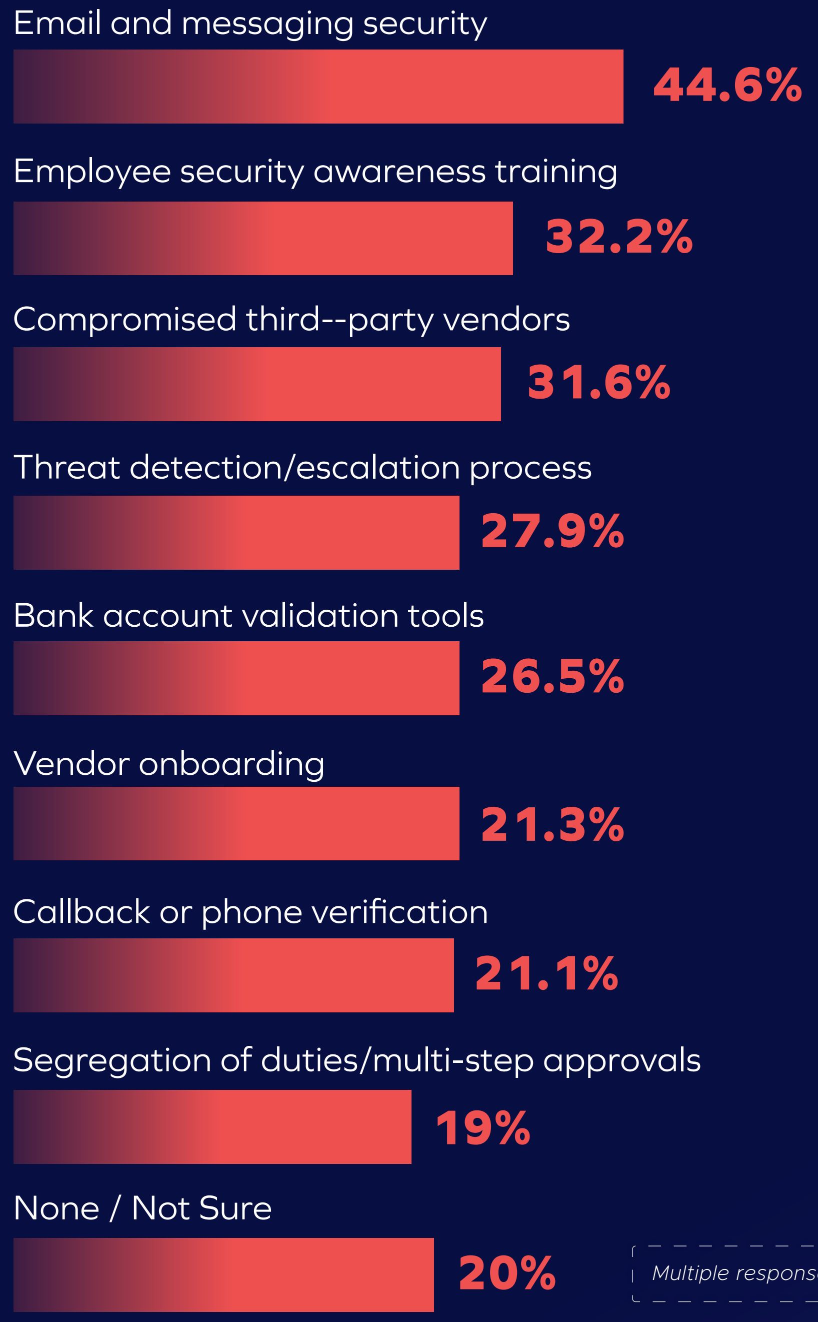
The Most Common Fraud Prevention Controls in Use /



Multiple responses allowed.

Even with these measures in place, breakdowns are common. Nearly 9 in 10 organizations said at least one control failed or was bypassed during a major incident.

Controls That Failed in a Significant Incident /



Multiple responses allowed.

When we asked how attackers got through, respondents pointed to a mix of process gaps and operational realities—many directly tied to siloed workflows. Even when policies were followed, they didn't always work.

Why It Matters /

Organizations are relying on controls with limitations in multi-system attacks. They perform as intended within their lane, but fraud no longer stays in one lane. Without defenses that bridge systems, signals, and teams, these gaps remain exactly where attackers aim.

Recommendations

Socially engineered fraud is no longer a "finance problem" or a "security problem." It's an enterprise-wide risk—supercharged by GenAI—that thrives in the seams between people, processes, and platforms. Addressing it requires a shift in both mindset and architecture.

1 *Collapse the Silos: Make Fraud a Shared Responsibility /*

Fraud prevention should not be split between departments or treated as an afterthought in either. Create a joint finance and security fraud council with shared KPIs, defined ownership for every stage of the incident lifecycle, and mandatory visibility into cross-team detections. GenAI-enabled fraud is too fast-moving for sequential handoffs. Both sides need to see the same threats, at the same time, in the same context.

2 *Upgrade from Single-System Controls to Cross-Platform Detection /*

Legacy safeguards, including email security, bank validation, and employee training are still valuable but insufficient alone. Deploy solutions that can correlate suspicious activity across ERP, messaging, vendor systems, and payment workflows in real time. AI-accelerated attacks are intentionally multi-system; your detection must be too.

3 *Build GenAI-Resilient Defenses /*

Fraud tactics are scaling faster than human review can keep up. Invest in behavioral AI and contextual monitoring that can flag anomalies across multiple systems, even when attackers convincingly mimic trusted communications, formats, or voices. GenAI must be met with AI that understands the organization's behavioral baseline and can detect deviations instantly.

4 *Measure and Report the True Impact of Fraud /*

Go beyond tallying direct financial losses. Track and report operational disruption, regulatory risk, and reputational damage. This fuller impact picture is essential to securing budget for GenAI-ready defenses that can scale and adapt as attack techniques evolve.

Methodology & Demographics

This report presents the key findings from Trustmi's Q2 2025 survey of 525 mid-to-senior level finance and cybersecurity professionals. The survey was designed to measure the prevalence and impact of socially engineered fraud, evaluate the collaboration between finance and security teams, and assess the effectiveness of current fraud prevention controls.

The research aimed to uncover how misalignment between these teams is driving financial risk in large enterprises.

Methodology /

Survey Period

Q2 2025

Audience

Mid-to-senior-level professionals in finance and cybersecurity roles.

Questionnaire

Structured, 25-question survey

Goal

Capture fresh, credible market data on the business impact of socially engineered fraud, gaps between teams, and the performance of traditional controls.

Organization Size

Over 50%
have more than 10,000 employees

63%
have revenues exceeding $5 Billion

Industries Represented

Industry	Share
Financial services & banking	**28.95%**
Technology & SaaS	**20.19%**
Healthcare & pharma	**9.9%**
Manufacturing	**9.14%**
Retail & eCommerce	**8%**

Roles

46.10%
Finance / Accounting
e.g., CFO, Accounts Payable Manager

45.33%
IT/Security
e.g., CISO, IT Director, Security Manager

This profile ensures the findings are representative of large, complex enterprises where socially engineered fraud presents both immediate financial threats and longer-term operational risks.

Note: The sample was weighted toward security professionals, which may influence perceptions of ownership and responsibility for fraud prevention. Percentages for multi-select questions may sum to over 100%.

Conclusion

The data is clear: socially engineered fraud isn’t just slipping past outdated controls but rather it's moving through the gaps between them.

In the GenAI era, those seams are widening. Attackers can now generate personalized, credible, and coordinated fraud campaigns at scale. They mimic trusted vendors, employees, and executives while jumping between systems to avoid detection. These are not static threats; they are adaptive, multi-step operations designed to exploit complexity and misalignment.

The single biggest vulnerability isn’t in the technology stack alone. The Trustmi 2025 Socially Engineered Fraud & Risk Report found that finance and security leaders were nearly evenly split on who should own fraud prevention. As long as fraud prevention is split by silos, enterprises will remain vulnerable to attacks that no one team sees from start to finish. Enterprises that treat fraud as a single-team problem will keep losing ground. The ones that win will close the distance: collapsing silos, unifying visibility, and coordinating response so there’s no “somewhere else” for the attack to hide.

About Trustmi

Trustmi is the only Behavioral AI security solution that empowers IT security and finance teams to prevent socially engineered fraud and payment errors before money moves.

By analyzing behavior across email, financial systems, and workflows, Trustmi detects socially engineered threats like BEC, impersonation, and vendor manipulation—attacks traditional tools miss.

Our end-to-end platform integrates seamlessly into existing systems, securing every B2B payment and ensuring funds reach the right destination—protecting people, processes, and the bottom line.

Visit us at
trustmi.ai

Regain Trust

Eliminate Socially Engineered Fraud

✓ **Prevents** *Fraud Losses*

✓ **Improves** *Efficiency & Control*

✓ **Reduces** *Costly Errors*

✓ **Strengthens** *Audit Readiness*