PAYMENT SECURITY REPORT

A focused look at today's fraud environment and the technologies treasury teams use to secure transactions, safeguard liquidity, and maintain control in real time.

Trustmi

Strategic Treasurer

1ST EDITION

This special edition provides an exclusive look at the solution set offered by Trustmi.

About the Payment Security Report

This inaugural edition of the Payment Security Report reflects Strategic Treasurer's recognition that payment protection has developed into a distinct discipline within corporate finance. As payment infrastructures expand and specialized security technologies emerge, treasury teams are increasingly asked to evaluate tools, coordinate controls across departments, and ensure that payment safeguards operate effectively within complex operational environments.

The Payment Security Report was created to provide focused insight into this evolving domain. It examines the structural foundations of payment protection alongside the technologies and services designed to strengthen it. We hope this publication equips treasury and finance leaders with practical perspective as they build more resilient and coordinated payment security programs.

TABLE OF CONTENTS

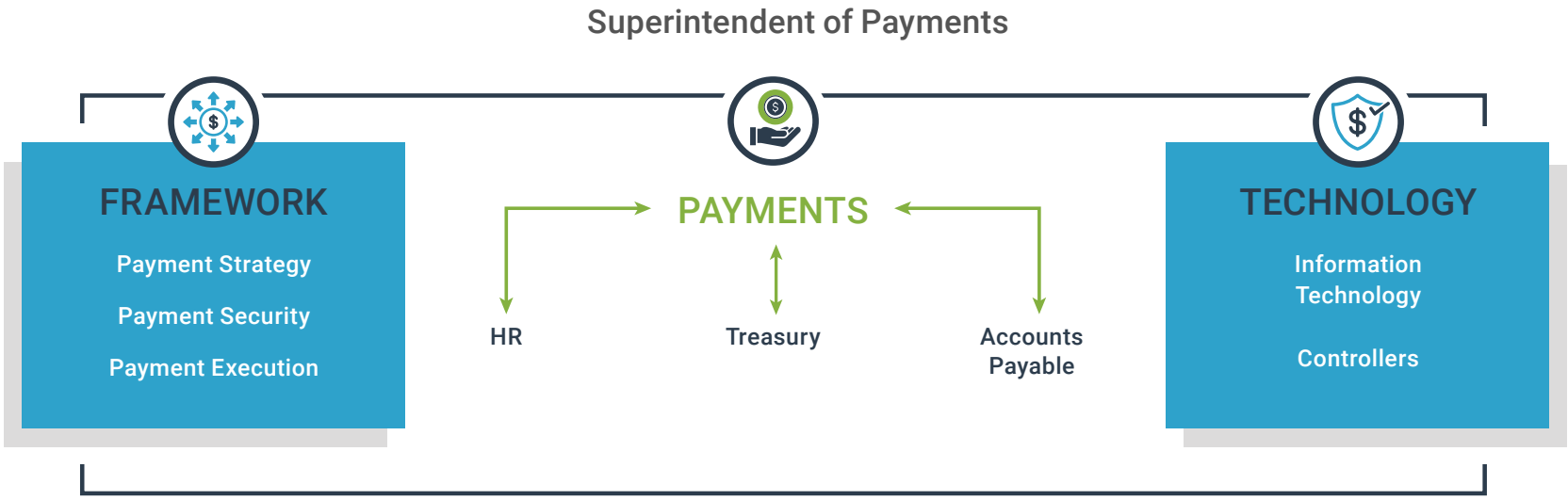
INTRODUCTION

The corporate treasury function now sits at the center of the organization's payment ecosystem, not only overseeing how funds move but also how they are protected. While IT and cybersecurity teams safeguard networks and infrastructure, the rising scale, speed, and sophistication of payments fraud have made one reality clear: transactional security requires coordinated oversight from the function with end-to-end visibility into payment flows. Increasingly, that role belongs to treasury, acting as the superintendent of payments.

This shift reflects a broader transformation in the payment environment. As faster payment rails expand and attackers deploy more adaptive tactics, securing payments has become a dynamic and ongoing discipline rather than a static set of controls. Treasury is no longer tasked solely with executing payments efficiently and accurately. It is expected to ensure that payment structures, processes, services, technologies, and people operate together within a coherent and resilient control framework.

The Payment Security Report addresses this imperative through a treasury-centered examination of fraud dynamics, defensive strategies, and the technologies designed to safeguard payment flows. The report explores the evolving threat landscape and the architectural approaches required to mitigate it. From validation protocols and monitoring services to behavioral analytics, automation, and increasingly specialized standalone payment security solutions, the report highlights the expanding range of tools available to strengthen defenses against both persistent and emerging fraud tactics.

This publication is structured to help treasury and finance professionals assess their organization's security posture and identify practical paths forward. It begins with an examination of the risk environment and criminal methodologies, then outlines layered methods of protecting payments, including structural, procedural, and technological safeguards. The final section provides a focused look at the security solutions offered by Trustmi.



PAYMENT SECURITY AS A STRATEGIC PRIORITY

Payment security has become a core strategic responsibility for treasury. As payment infrastructures accelerate and interconnect, and as fraud tactics continue to evolve, the risk profile surrounding transactions has intensified.

Two forces shape this environment: the transformation of how payments are executed and the escalation of threats targeting them. Positioned at the center of enterprise payment flows, treasury must address these pressures with structured oversight and coordinated controls. What follows is an examination of treasury's role, the risk environment, and the criminal playbook.

The Superintendent: Treasury's Expanding Role in a Changing Payment Environment

In today's corporate landscape, treasury is increasingly positioned as the superintendent of payment security. Like a superintendent overseeing a school system, treasury is not expected to perform every operational task or control every system directly. Instead, it carries responsibility for oversight, coordination, and accountability.

That oversight exists alongside other critical roles: IT and the CISO are responsible for securing infrastructure, networks, and endpoints, providing the technical foundation on which payment systems run. Accounts payable and payroll teams stand on the front lines of payment security as they carry out payment activities. Procurement influences onboarding and vendor data quality, while senior executives set governance priorities and tone, particularly around urgency, escalation, and exception handling. Each role contributes to payment security from a different vantage point, and weaknesses in any one area can introduce risk.

Treasury's position sits across these functions. It has visibility into how payments move end to end, where handoffs create exposure, and how overarching organizational security policies play into the equation. This perspective allows treasury to align controls across teams and identify gaps that may not be visible within individual departments. In its role as superintendent, treasury helps ensure that payment security is not fragmented by function, but coordinated as a system, with clear ownership, shared accountability, and controls that work together rather than in isolation.

As payment infrastructures accelerate and integrate more deeply across systems and departments, the superintendent role becomes more demanding and more consequential. Controls that once operated within manageable timelines and siloed processes must now function across compressed settlement windows and expanding attack surfaces. For treasury professionals, understanding the progression of this evolving risk landscape is essential, not only to appreciate the scale of the challenge but to shape an effective and coordinated response before the newest threats come knocking at the door.

Risk Environment

The payment risk landscape is not simply shifting. It is expanding. New rails, technologies, and attack methods emerge while legacy fraud schemes remain active and effective. Treasury therefore faces a growing threat environment in which advanced tactics layer onto longstanding ones, increasing complexity and sustained pressure on payment processes.

Attack methods themselves are becoming more sophisticated. Artificial intelligence is enabling impersonation schemes, automated reconnaissance, and highly tailored social engineering at scale. Synthetic identities, deepfakes, and convincingly crafted phishing messages are increasingly difficult to distinguish from legitimate communications. These developments do not replace traditional fraud methods such as business email compromise, credential theft, and account manipulation. Instead, they compound them, creating a layered and cumulative threat environment.

At the same time, the mechanics of payments are evolving. Faster payment rails such as FedNow and RTP settle transactions in seconds, reducing the opportunity for post-release intervention and shifting emphasis toward preventive controls. Meanwhile, the GENIUS Act has established a framework under which payment stablecoins may become viable for corporations, expanding activity across emerging digital asset rails. While these instruments promise efficiency and liquidity benefits, they also introduce new

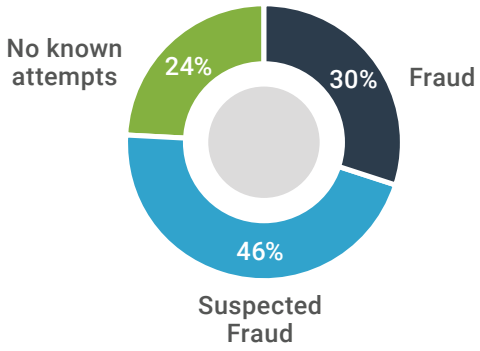
exposure vectors, from issuer solvency considerations to evolving regulatory interpretation.

Expanded integration across ERP systems, banks, and third-party platforms further increases connectivity and, with it, potential access points that must be governed carefully. API-based workflows and embedded finance models improve efficiency and scalability but also accelerate transaction flows, requiring disciplined oversight to prevent control gaps.

Each of these areas stacks on top of the others to create an ever-expanding risk environment. Findings from Strategic Treasurer's 2025 Treasury Fraud & Controls Survey reinforce this reality:

- Seventy-six percent of organizations experienced either fraud or suspected fraud in the previous year.
- Seventy-seven percent saw the threat level of fraud as having increased in the past year, with almost all others viewing it as steady and only 2% suggesting a decrease.
- Twenty-two percent plan to spend more on treasury fraud prevention and controls than in prior years, with over three-quarters of those citing management concern about the threat level as a primary driver.
- Business email compromise was the most frequently attempted fraud type and the second most frequent to result in loss. Payment diversion, involving changes to payment details on an invoice, was the most frequently successful attack type, with 11% of respondents experiencing a loss.
- Fourteen percent encountered synthetic identity fraud, and 30% reported fraud attempts involving AI-generated content. In both questions, however, around a third of respondents could only say they were unsure.

In the past twelve months, we have experienced _____[1]



In this environment, treasury must lead the organization through an increasingly compressed and technologically complex risk landscape. With visibility across payment flows and accountability for liquidity stewardship, treasury translates evolving threats into coordinated policies, structured controls, and disciplined execution across departments. As fraud methods accelerate and payment infrastructures evolve, treasury's leadership must ensure security is proactive and not just reactive.

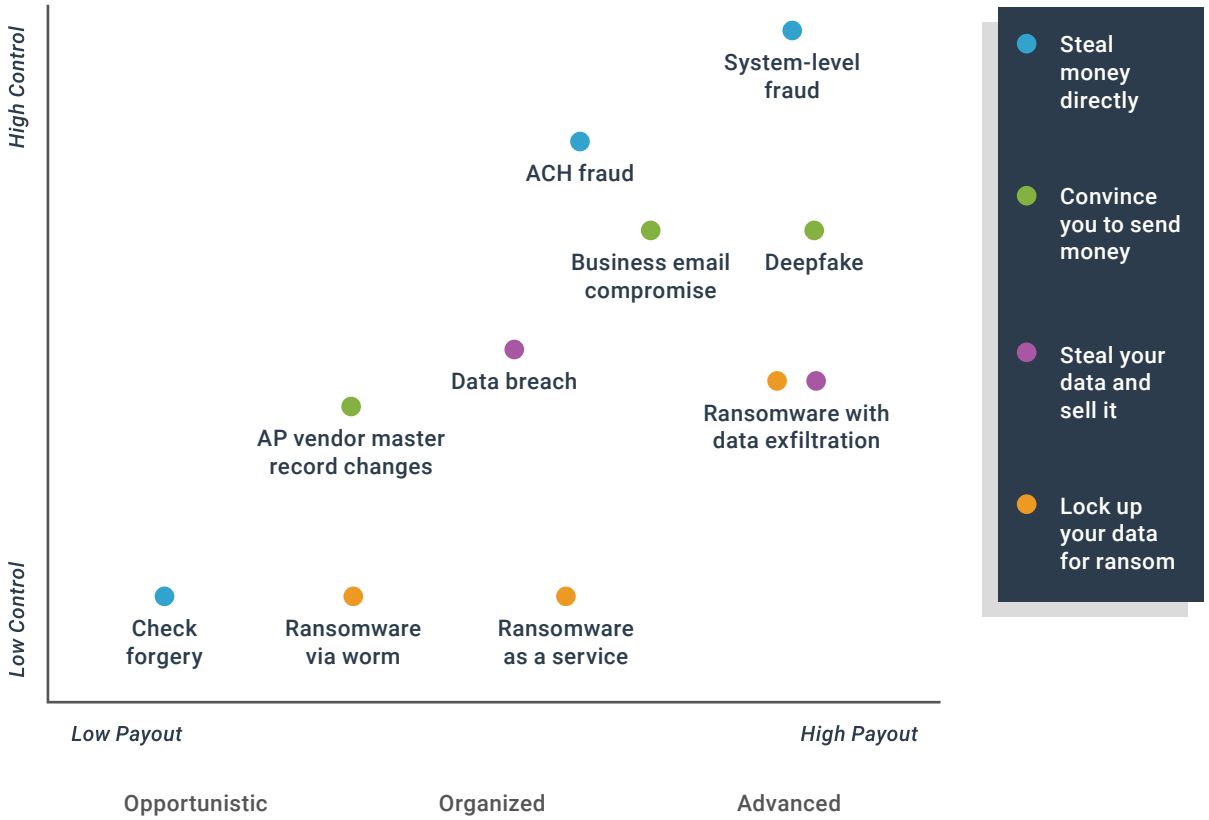
The Criminal Playbook

Fraud tactics are diverse and, in many ways, unpredictable, but most fall into one of four categories. Criminals are likely to begin with the most direct path to funds. As barriers rise against direct methods, fraud shifts to less direct attempts. This progression can be understood as a layered playbook. In some cases, various approaches are combined to increase pressure and maximize payout. Understanding this structure helps treasury teams recognize not only the types of attacks being used, but the logic behind their deployment and evolution.

1. **If they can steal funds directly, they will.**
   Direct theft remains a primary objective. Attackers target systems, intercept files, and exploit vulnerabilities in payment workflows to divert legitimate transactions. Traditional malware, file manipulation, and account takeover attacks fall in this category. Increasingly, criminals seek out integration points between ERPs, treasury systems, and bank portals. These points enable speed and efficiency through automation, but they must be paired with appropriate controls to ensure resilience.

2. **If they cannot steal directly, they try to convince you to send it.**
   If you make system-level theft too difficult, you will instead encounter social engineering. BEC remains the most commonly encountered approach, with criminals using spoofed emails, falsified domains, or impersonated vendors to generate urgency. AI has made these deceptions more convincing and automated, allowing attackers to mirror writing styles, voices, or even generate video impersonations of trusted figures. Tactics such as vishing (voice phishing) and smishing (SMS-based fraud) extend the attack surface further, particularly when internal

The Criminal Playbook



processes are inconsistent or overly reliant on informal communications.

3. **If they cannot convince you to send funds, they try to steal data.**
   Sensitive data such as credentials, payment templates, and vendor records can be monetized or leveraged in future attacks.

Criminals often gather this information through persistent surveillance or low-profile intrusions, especially in environments where logging and visibility are limited. The goal may be delayed but no less strategic: collecting enough internal detail to craft more credible future intrusions or to sell that access to others.

4. **If they cannot steal data, they lock it up for ransom.**
   Ransomware encrypts critical systems and demands payment for restoration. Often paired with data theft, this two-pronged tactic increases pressure on the organization. Even if treasury systems are not the direct entry point, they are affected when payments cannot be executed, files are compromised, or sensitive data becomes leverage.

These layers are not always isolated. A single incident may involve impersonation, credential harvesting, and malicious software all operating together. The blending of standard tactics with newer tools such as artificial intelligence has made it more difficult for treasury and security teams to distinguish real from fraudulent or urgent from fabricated.

Treasury's unique vantage point, which includes its oversight of payment workflows and its knowledge of how funds move through the organization, positions it as a key player in both recognizing these threats and selecting the right tools to address them. This environment of adaptive, multi-channel attacks has accelerated the need for purpose-built security solutions. General controls are no longer sufficient in this environment, accelerating the need for modern tools and dedicated security solutions.

STRATEGIC IMPERATIVE: CONTINUAL DEFENSIVE IMPROVEMENT

Payment security is not a project to be completed or a control set to be finalized. It is an ongoing discipline that must evolve at least as quickly as the risks it is designed to address. This section examines why continual improvement is essential in the current environment and how treasury can sustain an adaptive posture that keeps pace with both emerging and persistent threats.

Rationale: Why Static Security Fails

While fraud tactics evolve quickly, treasury environments are typically structured around periodic updates, audit cycles, and defined workflows. This creates an inherent gap between the pace of threat escalation and the speed at which most defenses are reassessed.

Controls that seemed paranoid last year may become part of the standard of good corporate conduct next year. As attackers identify new vulnerabilities and attack methods, they flood the corporate world with these new fraud attempts, hoping to catch those who fail to adapt quickly enough. Criminals often focus their efforts where defenses appear weakest or most out of date, making security an area where keeping up with peers is a meaningful part of staying protected.

Has your organization seen fraud attempts involving AI-generated content (e.g., documents, voice, video)?[1]

For treasury, this means defensive posture cannot be anchored to a fixed control set. Continuous reassessment is required whenever the threshold of acceptable protection shifts.

At the same time, updated controls cannot focus solely on the newest threat. Emerging technologies and AI-enhanced tactics demand focused attention, but with most losses still attributable to longstanding fraud schemes such as BEC, credential theft, and payment diversion, controls must layer to match the layering of risks.

Losses erode confidence, consume investigative resources, and damage trust across internal and external stakeholders. Treasury's mandate to safeguard liquidity carries an implicit expectation that its control framework evolves as risks evolve. Continual improvement is the only sustainable response to a threat landscape that both accelerates and accumulates.

Environment: Payment Rail Defenses

Continual defensive improvement requires more than tracking new fraud tactics. It demands an understanding of how your own systems and payment rails shape exposure. Each rail carries distinct settlement mechanics, timing structures, security features, and regulatory expectations. As organizations diversify their payment activity and look to adopt

new rails, defensive assumptions must be revisited accordingly.

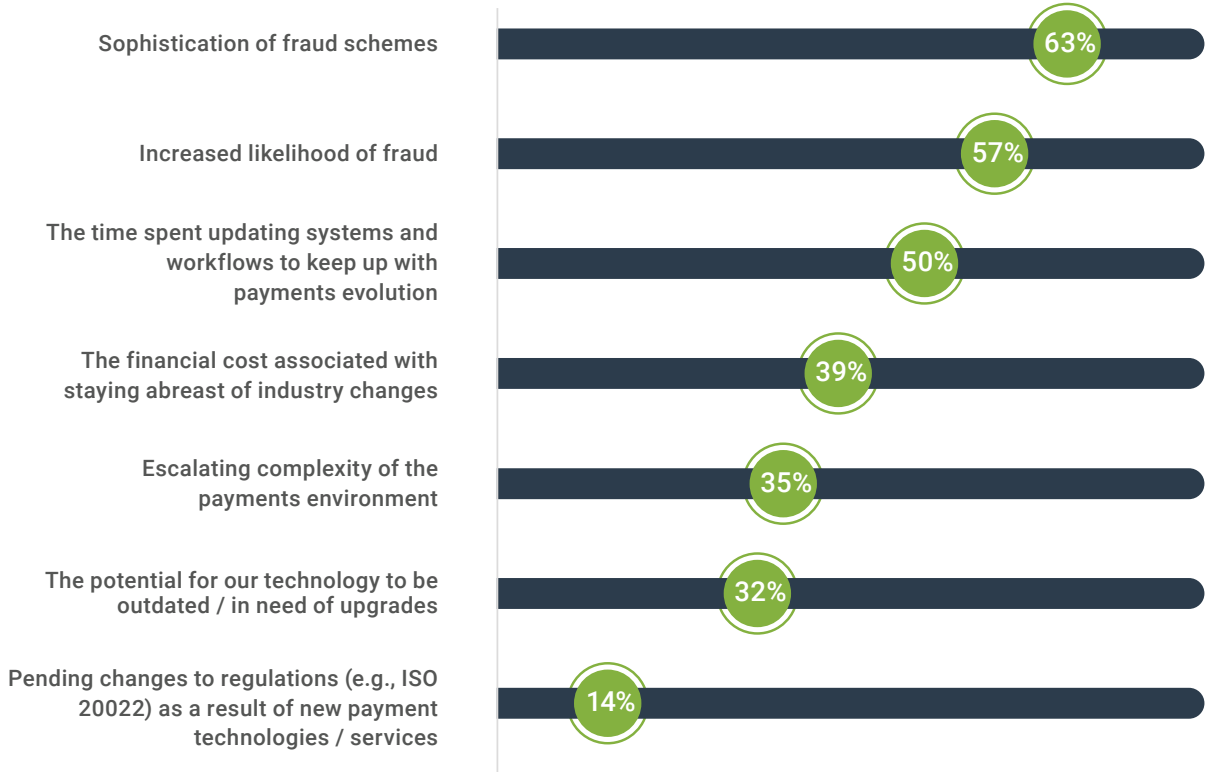
Real-time payment networks, such as the RTP® network and the FedNow® Service, illustrate how infrastructure changes alter control requirements. Immediate settlement and continuous availability introduce valuable operational efficiency, but they typically eliminate the possibility of post-release intervention. Preventative controls, including multi-factor authentication, validation, and always-on monitoring, become foundational rather than supplemental.

New and emerging channels further expand the defensive landscape. Tokenized payment methods and regulated stablecoins may offer speed and transparency advantages, yet they introduce governance needs, provider risk, and integration considerations that must be assessed continuously as adoption grows. In parallel, API-based payment initiation and third-party platform integration increase the number of endpoints through which payment data can be accessed or altered.

Even while the expanding landscape of payment rails draws concern and attention, traditional rails continue to present different but equally consequential exposure profiles and attendant security requirements. The ACH network, with its batch processing and reliance on static account data, remains a frequent fraud target. Nacha's account validation requirements for first-time payments reinforce the need for disciplined onboarding and change management. Card programs introduce decentralized usage and require strong controls over card data, including PCI-DSS compliance when card information is stored or transmitted within organizational systems, along with transaction-level oversight. Wire transfers and Swift-based messaging, often higher in value, depend heavily on credential integrity, segregation of duties, and outbound instruction validation, even with network-level safeguards such as the Swift Customer Security Programme in place.

As payment infrastructures diversify, the control environment cannot remain anchored to the dominant rail of the past. Defensive design must be rail-aware and adaptable. Diversification of payment channels will continue to accelerate, and recalibration of controls is not optional. In this environment, it is a necessary component of maintaining resilient, enterprise-wide payment security.

What are your TOP THREE concerns regarding change of payments technology and innovation? (Select three)[2]



METHODS OF PROTECTING PAYMENTS

Payment security plays out across five core areas: account structure, external services, operational processes, the human element, and enabling technologies. Each represents a distinct but interconnected layer of defense.

This section explores the first four of these areas, showing how treasury can shape the company's security posture through structural design, service selection, process discipline, and training. Because of the growing complexity of the threat environment and the expanding role of specialized tools, the fifth category (technology) is addressed in greater depth in its own section afterward.

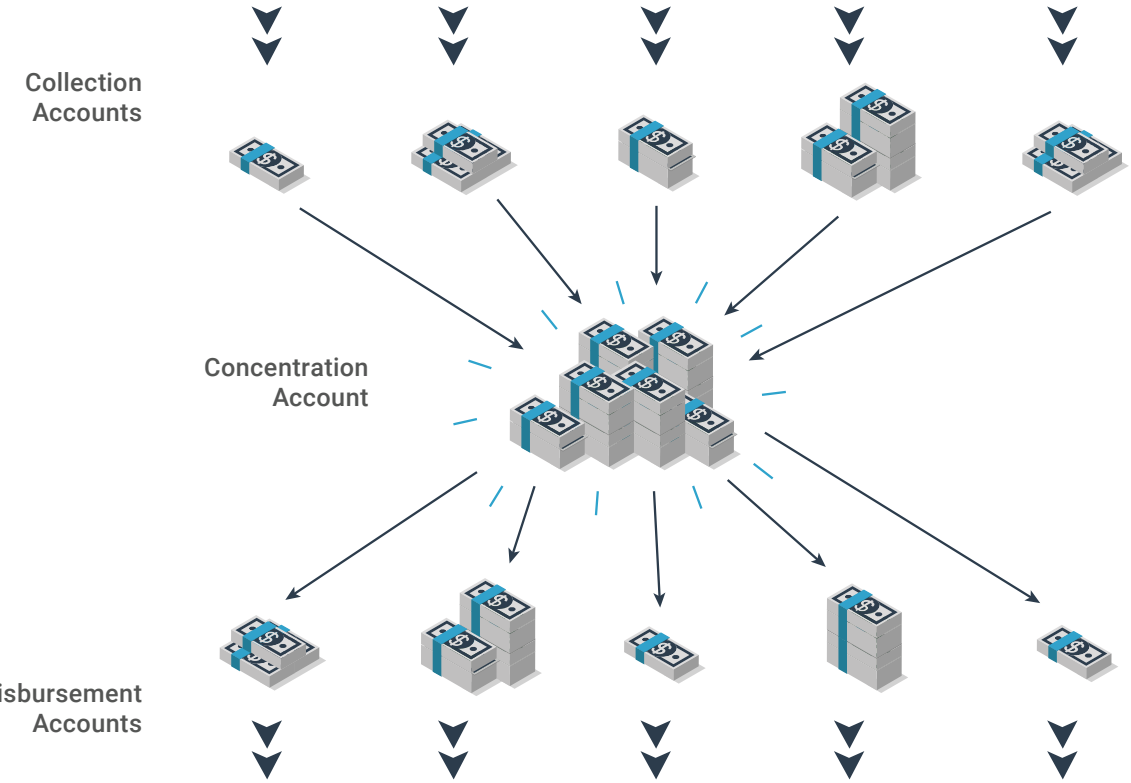
Structure

A deliberate, well-segmented account structure is one of treasury's most foundational tools for reducing payment risk. Assigning separate accounts for separate purposes limits the potential impact of fraud and makes unauthorized activity easier to detect. These distinctions may be as simple as separating disbursement accounts from collection accounts, or they may be more detailed, with separate accounts for different functions (AP, payroll, etc.) or for checks vs. ACH disbursements. Separating activity clearly in this way helps teams identify and trace irregularities quickly and reduce the likelihood that a single compromise will affect multiple payment types.

Zero-balance account (ZBA) structures further support control by minimizing idle balances in operational accounts. Funds are swept into or out of sub-accounts as needed, ensuring that only the precise amount required is available at any given time. This limits the opportunity for misuse.

At a high level, concentration or header account models extend these benefits on a large scale by enabling centralized oversight across a distributed account environment. Treasury can retain visibility into enterprise-wide payment flows while isolating operational access at the subsidiary or business unit level.

Structural choices can also support security technology by clarifying where controls should apply. Defined account roles and consistent design make it easier to implement rules, set limits, and automate



control logic within security platforms. This helps ensure that preventive measures align with how funds actually move through the organization.

More than what the structural choices are, it matters that treasury is intentional and thoughtful in laying the structure out. Organizational size, location, industry, and many other factors can all play into the structural needs and the areas of most vulnerability. Treasury's role is to assess the full picture and find ways to implement structure that allows both operations and security measures to function smoothly.

Services

External service providers are an essential part of treasury's payment security strategy. Banks and fintechs offer technology-enabled controls that operate at key handoff points in the payment lifecycle where internal oversight may not reach or where real-time responsiveness is critical. These solutions reinforce the organization's defenses by layering in independent validation, anomaly detection, and fraud prevention capabilities beyond core systems.

At the transaction level, services such as positive pay, file validation, and dual-approval workflows help ensure that payment instructions have not been altered or spoofed. These tools use automation to surface irregularities that might otherwise go unnoticed, especially in high-volume environments. By applying scrutiny at the point of release, they give treasury an added opportunity to identify and stop potentially fraudulent activity.

Validation and confirmation services focus on verifying the recipient side of each transaction, reducing the risk of funds being misdirected. These services are increasingly critical as impersonation schemes become more convincing and more common.

Some services also operate at the community level, using shared intelligence to detect broader patterns of fraud. Banks and fintech providers may flag high-risk transactions, unusual routing behaviors, or suspect counterparties based on activity observed across their platforms. These broader insights help treasury teams stay alert to risks that may not yet have surfaced within their own organization.

In an era of faster payments and an increasing need to catch more types of fraud before they happen, these external services are increasingly becoming a vital layer of protection. Teams that leverage them typically find that they pay for themselves rapidly.

Processes

Payment security depends not only on having controls in place, but on how those controls are implemented within day-to-day workflows. Processes must be designed deliberately, with awareness of upstream data inputs, downstream settlement implications, and the operational pressures that influence behavior. A control that disrupts critical timelines or creates friction without clarity is more likely to be circumvented than followed.

Fraud attempts frequently exploit process transitions, particularly where payment instructions are initiated, modified, or released. The onboarding of new payees and changes to existing vendor or employee payment details remain among the most vulnerable touchpoints. Effective process design requires independent verification of account instructions, clearly defined approval layers, and documented workflows that reduce ambiguity. Separation of duties between preparation and release is foundational.

At the same time, processes must account for human behavior. Controls only work if they are used and followed, and it is often possible to circumvent safeguards when processes are manual. Under deadline pressure or routine familiarity, individuals may shortcut verification steps or override warnings. Regardless of the motivation, this increases vulnerability.

This is where technology strengthens process integrity. When approval thresholds, authentication requirements, and validation checks are embedded directly into payment systems, they become an enforced part of the workflow. Technology does not replace well-designed processes, but it can support them by reducing the opportunity for circumvention and by creating audit visibility into how controls are executed.

Thoughtful process architecture therefore sits at the intersection of governance and technology. It allows treasury to align organizational priorities with secure execution, ensuring that payment workflows are not only documented but structured in ways that make secure behavior the default.

People

In a layered payment security model, the human element is integral. The classic image of payment fraud may be a hacker whose technical skills allow them to penetrate systems, but successful fraud schemes are

usually more about personal manipulation and social engineering. As the superintendent, treasury carries a responsibility for ensuring that all individuals involved in payment activity across the organization are equipped to recognize and resist those pressures.

Security awareness must extend to every individual involved in payment processes. Training should reflect the up-to-date realities of financial operations, focusing on the tactics used to target those functions, including impersonation, altered payment instructions, and attempts to bypass established approval paths. Individuals operating at every control point must understand both the mechanics of fraud and the rationale behind the safeguards embedded in their workflows.

Treasury's leadership must also help foster a culture in which verification is expected and escalation is supported. Employees across departments must be confident that they are authorized to pause and question any situation that appears inconsistent, even when urgent instructions seem to come from management or executives.

Technology strengthens this human layer when it is configured thoughtfully. Embedded approval logic, authentication requirements, validation checks, and system-enforced audit trails reduce reliance on memory and individual vigilance alone while creating visibility into how decisions are made. Rather than replacing judgment, well-designed systems guide it, making secure behavior easier to execute, harder to bypass, and traceable when exceptions occur.

As superintendent of payments, treasury's role is to align these elements. Secure payment environments are created not only through tools and policies, but through coordination across governance, systems, processes, and the individuals who carry them out.

When the broader organization is trained, empowered, and supported by embedded controls, the human layer shifts from a vulnerability to an adaptive and resilient component of enterprise payment security.

TECHNOLOGY AS A STRATEGIC SECURITY IMPROVEMENT

Technology has become central to how organizations execute, monitor, and protect payments. As transaction volumes increase, payment channels diversify, and fraud tactics accelerate, manual oversight and policy documentation alone cannot sustain effective control. Security expectations must be translated into system-enforced logic that operates consistently across entities, geographies, and rails.

Technology is no longer an operational convenience or a back-office enhancement. It has become a primary mechanism through which payment governance is implemented at scale. Approval hierarchies, segregation of duties, transaction validation, monitoring thresholds, and audit visibility are increasingly embedded within digital platforms. Understanding the technological foundations of payment security is therefore essential to understanding how modern defenses function.

Foundational Advances Shaping Payment Security

Several underlying technological developments have materially reshaped what is possible in payment security. While technological safeguards do not eliminate risk, they enable a level of monitoring, consistency, and adaptability that manual processes alone cannot achieve.

Artificial intelligence and machine learning have strengthened the ability to detect anomalies across large and complex datasets. Rather than relying solely on static rules, modern systems can analyze historical behavior across users, counterparties, payment types, and time patterns to establish behavioral baselines. When activity deviates meaningfully from those baselines, AI-enabled systems can identify those anomalies and alert users. Over time, these models can be refined to improve precision, reduce false positives, and adapt to new fraud patterns as they emerge.

Connectivity has also advanced significantly in recent years. API-based integrations now enable real-time or near-real-time data exchange among enterprise resource planning systems, treasury platforms, banks, and third-party services. This integration improves visibility across payment channels and reduces latency between transaction initiation, validation, and review. Where earlier environments depended heavily on batch updates and manual reconciliations, current architectures support faster confirmation and response.

Cloud infrastructure further enhances centralized oversight and scalability. Organizations can apply consistent security logic across distributed operations while maintaining consolidated reporting and control configuration. As payment activity expands across jurisdictions and entities, this centralized visibility becomes increasingly important to maintaining uniform standards.

Embedded policy engines and configurable control frameworks allow treasury to codify governance requirements directly into workflows. Approval routing, transaction limits, and exception triggers can be defined systematically rather than informally enforced. Detailed audit trails record user actions, overrides, approvals, and system responses, strengthening accountability and supporting investigation when anomalies occur.

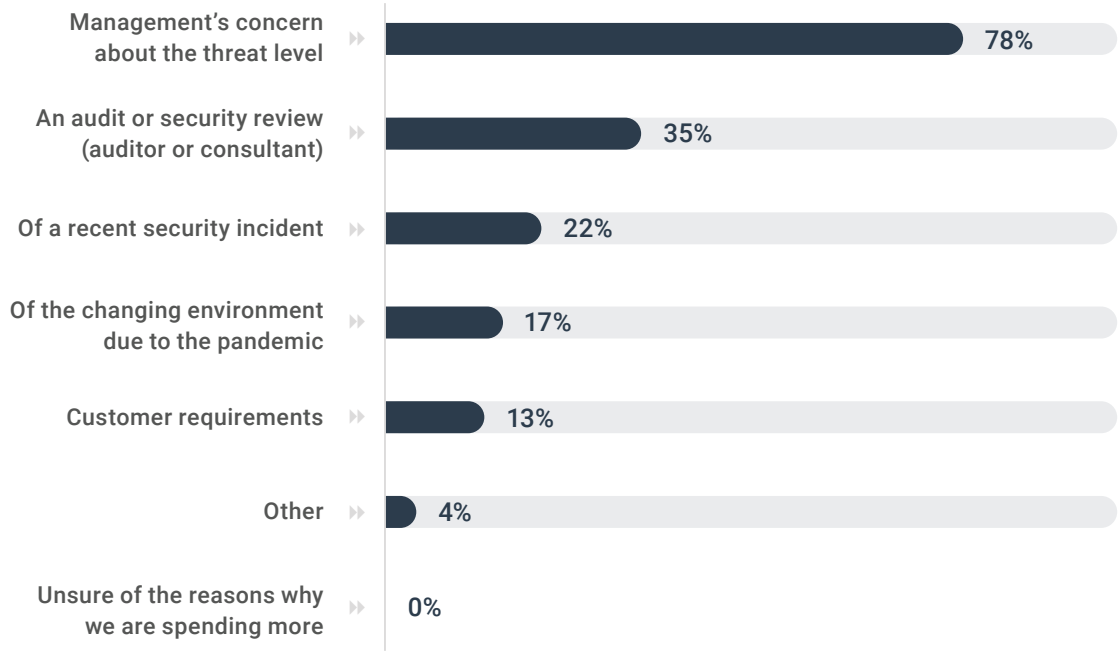
Taken together, these advances are changing the security landscape. While some of these innovations are also driving new forms of fraud, they are simultaneously empowering defenses. The corporate world cannot allow itself to be worse equipped than its enemies.

The Expansion of Dedicated Payment Security Solutions

As these foundational technologies have matured, organizational expectations around payment security have evolved in parallel. Capabilities such as behavioral analytics and real-time integration are moving from theoretical advantage toward practical necessity, and treasury teams bear the burden of ensuring their companies are not falling behind.

Findings from the 2025 Treasury Fraud & Controls Survey indicate that 22% plan to spend more or significantly more on treasury fraud prevention, detection, and controls compared to prior years. Of those, 78% cite management's concern about the threat level as a major driver in increasing that spending. Thirty-five percent noted an audit or security

We plan to spend more on treasury fraud prevention, detection, and controls because: (Select all that apply)[1]



review as driving their spending, while 22% attributed it to a recent security incident. Clearly, treasury is feeling pressure from multiple quarters to strengthen defensive infrastructure.

The market response to this need has taken multiple forms. Many treasury management systems, enterprise platforms, and bank portals have enhanced embedded security features, integrating validation checks, behavioral monitoring, and risk scoring directly into payment workflows. At the same time, specialized and standalone payment security solutions have emerged to address specific risk domains, including account validation, transaction screening, user behavior analytics, real-time alerting, and more. This is a growing area, with both new and established offerings meeting the market needs in varied ways.

This expansion signals increasing specialization within a maturing security ecosystem. As payment volumes rise, rails diversify, and attack methods accelerate, organizations require tools that can scale with complexity and adapt to new patterns of activity. The enabling technologies outlined in the prior section, including AI-driven analytics, API connectivity, and cloud infrastructure, have made this level of responsiveness achievable.

For treasury, the growth of dedicated payment security solutions introduces both opportunity and obligation. Opportunity lies in greater precision, faster detection, and improved control consistency. Obligation lies in learning and understanding the safeguards and technologies available, as well as in evaluating internal ecosystems and potential tools critically to ensure any additions align with governance standards, integrate effectively with existing workflows, and support real operational needs.

Treasury's Stewardship of Security Technology

Treasury's responsibility for security technology extends across its full lifecycle, from evaluation and selection through configuration, integration, and ongoing oversight. As superintendent of payments, treasury must ensure that technology choices align with organizational risk tolerance, operational realities, and the diversity of payment rails in use.

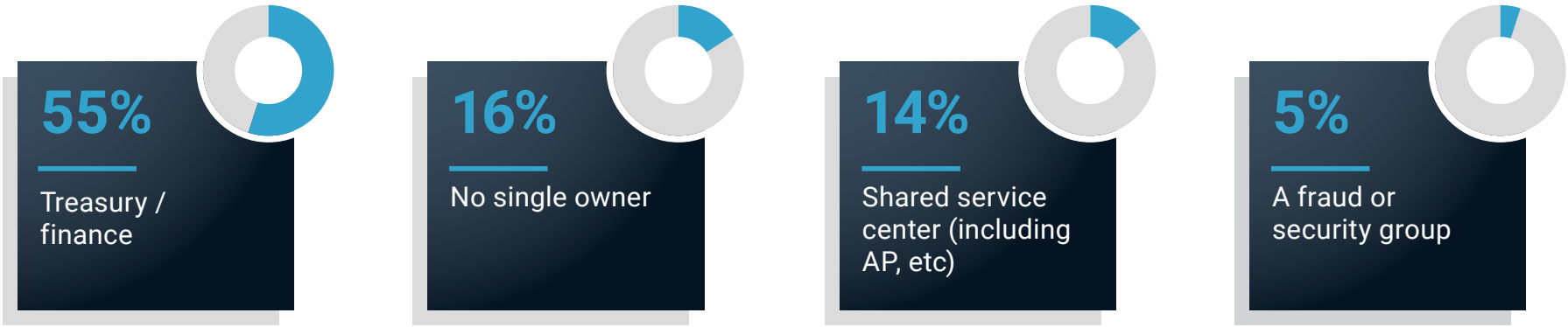
Tools must be assessed for their ability to support layered controls, integrate with existing platforms, and provide visibility across both emerging and persistent fraud risks. Once deployed, configuration becomes equally important. Thresholds, approval logic, authentication requirements, and alert parameters must reflect actual transaction patterns and business priorities. A poorly tuned system of any kind can generate noise, encourage workarounds, or create blind spots.

As payment volumes shift, rails expand, and fraud methods continue to evolve, control logic must

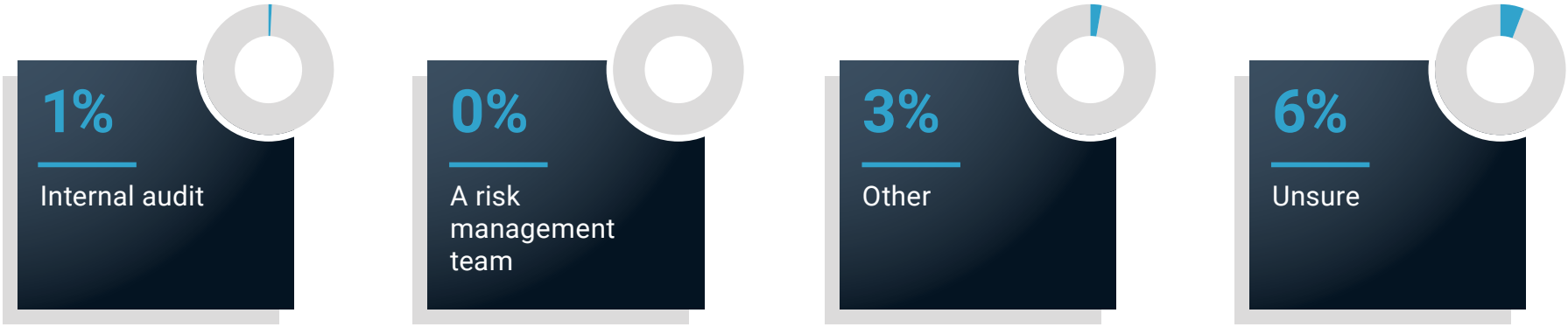
be reassessed. Behavioral baselines may need recalibration. Alert criteria may require refinement. Legacy fraud schemes must remain accounted for even as new tactics emerge. Technology that is not periodically reviewed holds the risk of becoming static in a dynamic environment.

Payment security will always be an ongoing process, not a project with an endpoint. Maintaining its effectiveness requires structured review and ongoing monitoring, which are examined more closely in the following section.

Who owns payment risk management in your organization?[1]



Treasury is already recognized as the superintendent of payments by the majority of companies.



KEEPING CURRENT: MONITORING FRAUD AND DEFENSES

The effectiveness of any payment security program depends on its ability to keep pace with change within the business, across its partner ecosystem, and throughout the broader threat landscape. Treasury's role does not end when controls are implemented or technology is deployed. It must maintain a continuous improvement loop, learning about what's changing in the broader environment and monitoring the ongoing effectiveness of internal efforts.

This section explores the practical mechanisms that support this vigilance: assessments, audits, and monitoring. It also looks at how treasury can structure its fraud strategy as an intentional, evolving, and focused program for long-term resilience. These practices strengthen internal safeguards and shape the selection and refinement of the tools the organization relies on to protect its payments.

Internal Security Assessments

Internal assessments are treasury's opportunity to proactively evaluate whether existing safeguards are still appropriate for the current environment. These reviews help identify control gaps, process misalignments, and shifts in exposure that may have emerged as the organization evolved or as fraud tactics changed. Assessments should be performed at least annually to ensure continued alignment between controls and the current risk landscape.

During these assessments, treasury should evaluate whether controls are being bypassed in practice, whether new technologies or processes have introduced unintended risks, and whether policies still match the organization's operational reality. Access governance is a critical component of this review. User entitlements should be examined to confirm that permissions align with current job responsibilities, that former employees are being removed promptly, and that segregation of duties remains intact as roles evolve.

In many organizations, assessments also inform investment decisions. When recurring gaps or emerging exposures are identified, treasury can determine whether adjustments are needed in technology, processes, or training. Over time, this approach allows the security program to evolve in a structured and deliberate way, keeping pace with the evolving environment.

Independent Payment Assessments and Audits

Where internal assessments allow treasury to review and refine controls on an ongoing basis, audits provide a structured and independent examination of the control environment. They evaluate whether payment security practices align with internal needs and external standards. Conducted at regular intervals, audits introduce disciplined external perspective into a function that can otherwise become accustomed to its own routines.

The primary value of an independent audit rests in its ability to surface blind spots. Control environments often appear sound from within, particularly when processes have operated without visible incident. Auditors may inventory payment flows, test assumptions, and review documentation in ways that challenge embedded habits and unexamined confidence. This scrutiny can reveal overlooked payment streams, gaps in approval workflows, inconsistencies in access management, weaknesses in documentation, or informal workarounds that undermine effectiveness.

Treasury plays a central role in supporting audit readiness. This includes maintaining clear records, aligning user permissions with payment responsibilities, and preserving traceability across systems. When approached constructively, audit results provide a structured basis for strengthening controls and correcting assumptions before they result in loss.

Monitoring

Monitoring offers treasury a way to maintain real-time or near-real-time visibility into its payment environment. While assessments and audits provide valuable periodic checkpoints, monitoring fills the gaps between those reviews, alerting teams to anomalies, unauthorized activity, or shifts in behavior as they occur. When implemented effectively, monitoring enables faster response times, reduces the window for fraud, and supports more agile decision-making.

Monitoring can take many forms. Some solutions flag abnormal transaction patterns based on behavioral analytics or past activity. Others track system access logs, user activity, permission changes, or deviations from established workflows. Monitoring may also involve alert configurations that trigger when certain conditions are met, such as a payment to a new beneficiary, an override of a dual-approval requirement, or the assignment of elevated user privileges.

Effective monitoring requires more than just technology. Treasury teams must define what normal access and transaction behavior look like in their environment and configure tools to surface relevant alerts without creating noise. Monitoring programs should also be reviewed regularly to ensure they remain aligned with evolving risks, systems, and business processes.

Intentional and Focused Security Programs

Assessments, audits, and monitoring provide mechanisms for staying current. What determines their effectiveness, however, is whether they operate within a coherent and sustained program of oversight. Without clear ownership and coordination, even well-designed reviews can become isolated exercises rather than drivers of improvement.

Treasury's role as superintendent requires more than participating in control activities. It requires ensuring that security efforts across systems, departments, and payment rails are aligned and cumulative. Findings from monitoring should inform assessments. Audit observations should shape configuration decisions. Technology investments should reflect identified control gaps rather than abstract capability trends.

When these elements operate independently, gaps persist. When they are connected, the security posture strengthens over time.

This programmatic discipline is especially important in a layered threat environment. New fraud techniques demand attention, but longstanding schemes continue to exploit process weaknesses and control gaps. An effective security program maintains coverage across both emerging and persistent exposures, recalibrating controls without abandoning foundational safeguards.

Ultimately, sustained payment security depends on continuity of oversight. Payment channels expand, personnel change, and technology evolves. A structured program ensures that responsibility does not fade and that adaptation remains deliberate rather than reactive. Through coordinated stewardship of people, processes, structures, and technology, treasury can maintain a resilient control environment capable of withstanding both acceleration and accumulation of fraud risk.

trustmi

Same Payment. Different Outcome.

The difference is stopping what traditional controls miss.

trustmi Behavioral AI

- Cross-System Visibility
- AI-Driven Decisions
- Automatic High-Risk Holds

Learn more at **trustmi.ai**

trustmi

trustmi.ai
info@trustmi.ai

See Trustmi in Action

Security Services

Services & Controls

Validation & Data Integrity

- ABA Validation ✓
- IBAN Validation ✓
- File Encryption ✓
- Hashed Payment (account information) ✓
- Hashed Payment File ✓

Access Control & Data Protection

- Tokenization ✓
- Biometric Authorization ○
- Multi-Factor Authentication (MFA) ✓

Validation

- Know Your Customer (KYC) ✓
- Governmental Checking (e.g., SoS records) ✓
- Onboarding Process Management ✓

Verification

- Direct Verification w/Counterparty ○
- Payee Account Ownership (e.g., entity name match) ✓
- Secure Bank Letters ✓
- Community Network Verification (inclusion, history) ✓
- Bank Network Verification (e.g., account owner) ✓

Confirmation and Authentication

- API Confirmations ○
- Open Banking Consent-Based Verification (API) ○
- Deposit Validation/Authentication (e.g., microdeposits) ✓
- Payee Matching, Positive Pay ✓

Rating

- Risk Scoring / Evaluation of Data Reliability ✓

Monitoring, Interdiction, and Investigation

Screening

- AML Screening ○
- Sanction Checking ✓

Monitoring & Detection

- Internal Threat Management ✓
- Anomaly Detection (data) ✓
- Anomaly Detection (behavioral analytics) ✓

Interdiction & Investigation

- Interdiction ✓
- Audit Trail Management ✓
- Activity Recording ✓
- Replay Management ✓

Confidence in Every Payment Decision

Treasury teams have more controls than ever, yet fraudulent payments still get approved.

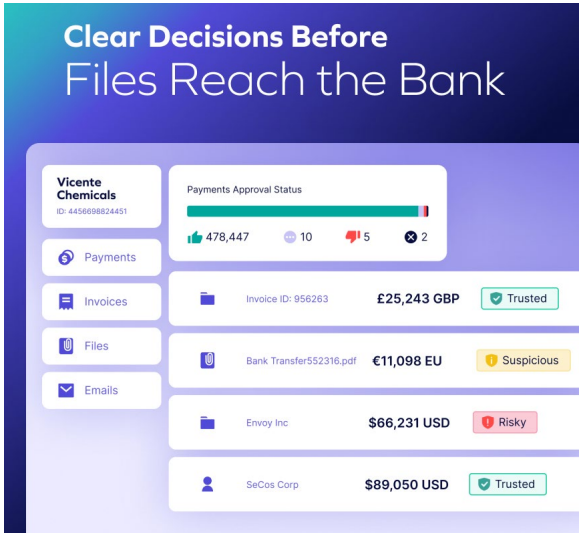
As payment environments grow more complex and fraud becomes more convincing, some risks are harder to detect through isolated checks alone. In a recent Trustmi benchmark analysis, **90% of fraudsters used bank-approved accounts.**

When trusted signals like bank validations can be misleading, Treasury needs more than verifications alone. As leaders push teams to improve efficiency with AI, Treasury needs smarter payment assurance before funds are released.

How Trustmi Blocks Risky Payments

Trustmi uses Behavioral AI to evaluate each payment before release across workflows, vendors, documents, accounts, approvals, and historical behavior. It confirms bank account ownership and authorized beneficiary details through a broader view than standalone verification checks.

With Trustmi, Treasury gains clear visibility into what matches expectations, what changed, and what needs attention before funds move.



What Treasury Teams Gain with Trustmi

Every capability below supports one objective: helping Treasury release only payments that are safe, accurate, and authorized.

Deliver Clear Decisions

SAFE / UNSAFE verdicts before files reach the bank.

Detect Exceptions & Hidden Risk

Analyzes payment behavior, workflow changes, vendor updates, and transaction context to flag suspicious or misdirected payments inside normal runs.

Analyze Every Payment in Every Run

Screens every payment in every batch, including thousands of transactions at once.

Confirm Trusted Payees & Beneficiaries

Helps verify bank account ownership, beneficiary details, and trusted payees before release.

Strengthen Approval Governance

Supports multi-signature approvals, oversight controls, and payment governance requirements.

Built for Speed, Control, & Confidence

Trustmi is built for Treasury teams that must move quickly while maintaining trust in every payment they release. It uses AI to surface high-risk payments, reduce manual review, and strengthen confidence before payments are released.

By surfacing the highest-risk transactions first, Trustmi reduces noise and helps Treasury focus time where judgment is needed most.

Connected Intelligence for Treasury

The controls Treasury relies on still matter, but attackers now design fraud to pass them by combining signals that appear trustworthy on their own.

Modern payment fraud often layers multiple tactics:

- 85% of attacks start in email—and go undetected

by email security
- 39% used fraudulent financial documents
- 90% of fraudsters use bank-approved accounts
- 59% used multiple coordinated tactics

The issue is no longer one failed control. It is multiple trusted signals creating false confidence.

That is why Treasury needs connected payment intelligence that evaluates risk across the full payment lifecycle.

Measurable Value for Treasury

When payment decisions are informed by the full picture, stronger protection can deliver clearer outcomes. From reducing losses to improving ROI, Trustmi helps organizations achieve measurable results.

Strong ROI

Customers have seen at least **10x ROI.**

Reduced Financial Losses

Average detected and prevented exposure of **$1.5M**.

Proven at Enterprise Scale

$240B in payments validated by Trustmi.

Modernization With Accountability

Adopt AI in a way that supports trust and governance.

Automatic Hold on High-Risk Payments

Trustmi stops high-risk payments before funds leave.

How Treasury Gains Back Time

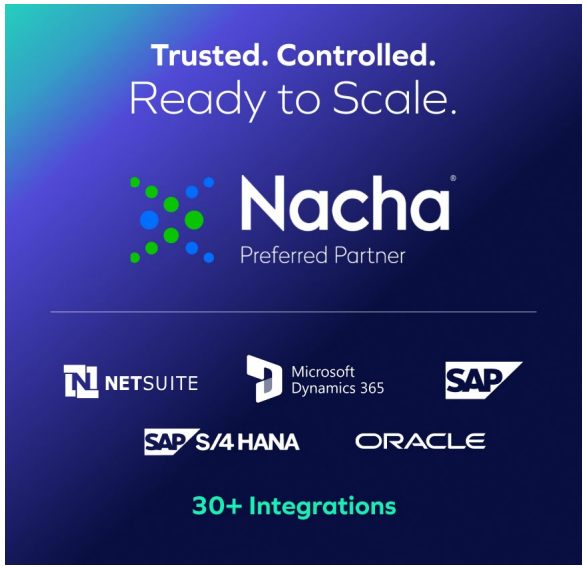
Value is measured in more than dollars. It is also measured in time returned to the people responsible for keeping payments moving.

> **"Before Trustmi, we investigated around 20 incidents a month. Now we investigate nearly zero."**
>
> **- Customer CISO**

When investigations drop from around 20 incidents a month to nearly zero, Treasury teams can reduce escalations, move payments faster, and spend less time resolving suspicious activity.

Bring Certainty to Every Payment

Treasury's role has never been more important. Teams



are expected to move quickly, maintain strong controls, and release payments with confidence in increasingly complex environments.

That requires more than process completion alone. It requires greater visibility into payment risk, trusted decision support, and confidence before funds move.

See how Trustmi helps Treasury reduce manual reviews while stopping risky payments at Trustmi.ai.

With fraud on the rise, every organization is being targeted.

Is your team ready for the next attack?

For an even more detailed look at payment security through the lens of operational discipline, download Strategic Treasurer's SECURE CLAMPS ebook. The ebook presents twelve foundational practices that help organizations structure and execute payments safely. Even as fraud tactics and technologies change, these core disciplines remain a consistent framework for strengthening payment security.

Download the ebook

SOURCES

1. 2025 Treasury Fraud & Controls Survey – Strategic Treasurer and Bottomline
2. 2024 Global Payments Survey – Strategic Treasurer and TIS

Strategic Treasurer was founded in 2004 by Craig Jeffery, a financial expert and trusted advisor to executive treasury teams since the early 1990s. Through advisory services and research, they serve companies, banks, and fintechs across the globe. This team of experienced senior treasury advisors are widely recognized and respected leaders throughout the industry. Known for their expertise in treasury technology, risk management, and working capital as well as cash management and banking operations, they efficiently identify issues, creatively explore ideas and options, and provide effective solutions and implementations for their clients.

strategictreasurer.com

info@strategictreasurer.com