BASEFUND

Trust in Transit

Safeguarding Financial Transactions 2025

Table of Contents

01 Executive Summary

The transaction security landscape has transformed dramatically in recent years, and 2025 finds us at a fascinating inflection point. Financial institutions are navigating a world where digital transactions have become the norm rather than the exception, with global digital payment volume increasing by 32% since 2023 alone.

The most prevalent threats aren't necessarily the most technically sophisticated. Business email compromise remains the number one risk to secure transactions, with our research showing that 68% of successful attacks begin with simple yet effective phishing attempts. These attacks target the human element of security, often bypassing technical safeguards through social engineering rather than complex hacking techniques.

As one CISO puts it: "The transaction security landscape in 2025 isn't just about stronger walls—it's about smarter systems that can adapt to threats we haven't even imagined yet."

For financial professionals, the path forward requires strategic investments in both technology and people.

While our data shows organizations with security awareness training experience fewer successful social engineering attacks, training alone simply isn't cutting it. Human error remains inevitable, which is why no transaction should be left to chance.

Basefund's position in this landscape is straightforward: stop fraud when money is in motion. Our platform provides an essential layer of protection for external transfers, ensuring funds reach their intended destination without falling victim to increasingly sophisticated scams.

The transaction security challenges of 2025 are substantial, but so are the opportunities to build more resilient, trusted financial systems. This report aims to provide you with a clear picture of where transaction security stands today and where it's headed tomorrow. Let's explore how we can navigate this landscape together.

02 **Introduction:** The Evolving Transaction Security Landscape

Defining Transaction Security

Transaction security encompasses far more than it did even a few years ago. Today, it refers to the comprehensive set of protocols, systems, and practices designed to protect financial transactions throughout their entire lifecycle—from initiation to final settlement. What makes modern transaction security distinct is its focus on protecting "money in motion"—those critical moments when funds are being transferred between accounts, which represent the highest point of vulnerability.

Transaction security now spans multiple domains:

- Identity verification and authentication of all transaction parties
- Protection of transaction data during transmission
- Validation of transaction integrity and legitimacy
- Defense against manipulation or interception during processing
- Confirmation of proper settlement

Unlike traditional security models that focused primarily on account protection, modern transaction security emphasizes the journey rather than just the endpoints. This shift recognizes that sophisticated threat actors increasingly target transactions during transit, when defenses are often at their weakest

Major Shifts in the Threat Landscape Since 2023

The transaction security landscape has undergone remarkable transformation since 2023, driven by several interconnected trends:

1. **The Rise of Hybrid Attack Chains**
   Rather than relying on pure technical exploits or social engineering alone, today's most successful attacks combine multiple approaches. A typical attack might begin with targeted phishing to establish initial account access, followed by technical manipulation of transaction systems, and conclude with social engineering to bypass final verification checks.

2. **The Democratization of Sophisticated Attack Tools**
   Advanced attack methodologies once limited to nation-states or elite cybercriminal organizations have become widely accessible. Open-source tools, criminal-as-a-service offerings, and generative AI have dramatically lowered barriers to entry for conducting sophisticated financial fraud.

3. **Business Email Compromise (BEC) Evolution**
   BEC attacks have evolved from crude impersonation attempts to highly sophisticated operations leveraging deep research, precise timing, and convincing pretext scenarios. With the adoption of generative AI, BEC attacks have become increasingly difficult to distinguish from legitimate communications.

4. **Growing Sophistication of Payment Misdirection**
   Attackers are increasingly focusing on payment misdirection tactics that exploit legitimate transaction processes. Rather than trying to breach secure systems, these attacks manipulate authorized users into sending funds to fraudulent destinations. These schemes often involve last-minute changes to payment instructions, creating false urgency, or using nearly identical domain names and account details that can easily go unnoticed during routine processing.

5. **The Human Element Remains the Weakest Link**
   Despite technological advances in transaction security, human decision-making continues to be the most vulnerable point in the security chain. Financial professionals operating under time pressure, with incomplete information, or lacking security awareness remain the primary target for attackers.

6. **The Insurance Gap for Money in Motion**
   A critical and often overlooked vulnerability in transaction security is the insurance gap. Unlike funds held in accounts, which typically benefit from FDIC or similar protections, money in transit via transfers has no comparable insurance safety net. Once a fraudulent transaction is completed, the funds are often unrecoverable, leaving businesses fully exposed to financial loss. This gap has made transaction fraud particularly attractive to cybercriminals, who know that successful attacks often result in permanent financial damage to their victims.

Growth of Digital Transactions: 2023-2025

The volume and value of digital transactions continue to grow exponentially, creating both opportunities and security challenges:

- Global digital payment volume increased 32% between 2023 and 2025, reaching $15.3 trillion annually
- Corporate-to-corporate payments now for 78% of all B2B transaction value, up from 61% in 2023

This dramatic growth in transaction volume creates significant security challenges as financial systems process more transactions than ever before, with each representing a potential point of vulnerability.

03 The Evolution of Transaction Design

The financial industry is rapidly moving away from rigid, standardized transaction structures toward flexible, purpose-built payment flows that match the unique needs of different transaction types. This shift represents both a significant opportunity and a notable security challenge.

Traditionally, financial transactions followed predetermined paths with limited flexibility, forcing businesses to adapt their operations to fit within these constraints. Today's landscape is dramatically different. Financial professionals gain the ability to design customized flows that align perfectly with their specific business requirements, creating more efficient processes while potentially introducing new security considerations.

Security Challenges in Customized Transaction Environments

While customizable transaction flows offer tremendous operational benefits, they also present unique security challenges:

- **Increased Surface Area for Attack**
  Each customization point represents a potential vulnerability. The more flexible and customizable a transaction flow, the more opportunities exist for manipulation if proper controls aren't in place.

- **Participant Verification Complexity**
  Custom flows often involve multiple participants, each requiring proper verification. As the number of participants increases, verification complexity grows exponentially.

- **Non-Standard Process Vulnerabilities**
  Custom processes may not benefit from the security hardening that comes with standardized, well-established transaction patterns, potentially creating unique security gaps.

- **Configuration Errors**
  The ability to customize transaction flows introduces the possibility of security-compromising configuration errors that wouldn't exist in more rigid systems.

- **Variable Security Requirements**
  Different transaction types require different security approaches. Without proper guidance, organizations may under-secure

Securing the Custom Transaction Era

Organizations building custom transaction flows require a comprehensive security approach that includes:

Bank Verification
Microdeposit verification and other bank validation techniques remain essential to confirm account ownership and prevent misdirected funds. These processes must be integrated seamlessly into transaction flows without creating undue friction.

Identity Verification for All Participants
Know Your Customer (KYC) principles must extend beyond direct customers to all transaction participants. Identity verification checks are particularly crucial for high-value or unusual transactions.

Role-Based Controls
Custom transaction flows should enforce appropriate separations of duty and role-based access, ensuring no single participant can compromise the entire process.

As transaction platforms evolve to provide greater customization options, organizations must balance flexibility with security. The most successful approaches will integrate robust security measures directly into the transaction design process, ensuring protection is built into the foundation of every custom flow rather than applied as an afterthought.

By embracing both the flexibility of custom transaction flows and comprehensive security measures, organizations can create payment processes that are both efficient and secure—allowing financial professionals to focus on business operations rather than security concerns.

04 Beyond Technology: The Human Element in Securing Transactions

While sophisticated technology plays a vital role in transaction security, the human element remains both the greatest vulnerability and the strongest potential defense. Financial professionals who understand transaction security risks can serve as an effective first line of defense, while those lacking awareness often become the entry point for fraud.

The most secure transaction platforms recognize this reality: technical controls alone cannot fully protect money in motion. Education must be viewed not as supplementary but as fundamental to a comprehensive transaction security strategy.

The Education Gap in Financial Security

Despite the critical importance of security awareness, a concerning education gap exists among financial professionals:

- 72% of finance team members receive less than two hours of security training annually
- Only 31% of businesses conduct specific training on securing external money transfers
- 84% of financial professionals report feeling uncertain about their ability to identify sophisticated payment fraud attempts
- 66% of organizations that experienced transaction fraud had no structured program for educating staff about security risks

This education gap creates a significant vulnerability, particularly as attackers increasingly target the human element rather than technical systems. As one security expert notes, "Most attackers don't try to break encryption anymore—they focus on breaking trust."

Effective Education Strategies for Transaction Security

Organizations that have successfully reduced transaction fraud through education share several common approaches:

Specific vs. General Security Training

Generic cybersecurity training has proven insufficient for addressing transaction-specific risks. Effective education programs focus on the particular vulnerabilities associated with money in motion, including:

- Recognizing signs of fraudulent payment change requests
- Verifying banking details through multiple channels
- Understanding the importance of account ownership verification
- Identifying the warning signs of business email compromise
- Following secure procedures for high-value transfers

Continuous Reinforcement vs. Annual Training

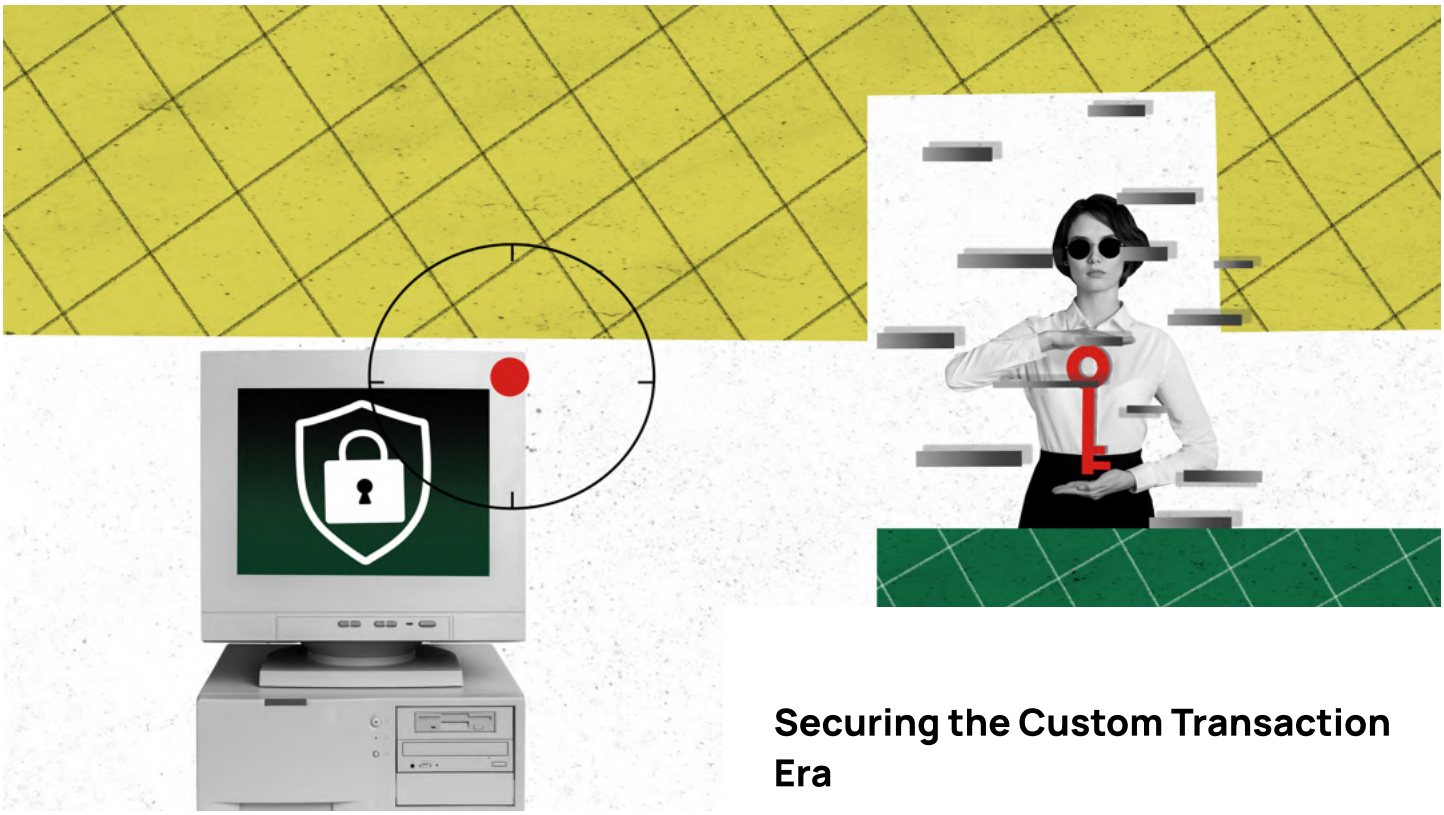
Transaction security awareness requires ongoing reinforcement rather than annual compliance-focused sessions. Leaders in this area provide:

- Brief monthly security updates highlighting new attack techniques
- Just-in-time reminders integrated into transaction workflows
- Regular sharing of relevant fraud attempt case studies
- Celebration and recognition of staff who identify and prevent fraud attempts

Clear, Actionable Guidance

The most effective education programs avoid vague advice like "be vigilant" in favor of specific, actionable guidance:

- Exactly which details to verify before approving payments
- Specific steps for confirming unusual transaction requests
- Clear escalation paths when suspicions arise
- Concrete verification procedures for new payment recipients
- Checklists for high-risk transactions



Building an Integrated Security Approach

The future lies in "security by design" – systems that incorporate protection as a fundamental element rather than an added layer:

- Automation for routine verification with human judgment for complex cases
- Default secure behaviors requiring no extra effort
- Automated account ownership verification
- Transaction workflows with embedded security controls

Securing the Custom Transaction Era

Organizations implementing this integrated approach see measurable improvements:

- 67% reduction in successful fraud attempts within six months
- 54% increase in fraud attempt reporting
- 82% improvement in identifying suspicious transactions
- 43% reduction in legitimate transaction approval time

This comprehensive approach recognizes human limitations while leveraging human strengths, creating a more sustainable strategy for protecting money in motion.

05 The Basefund Approach to Transaction Security

Protecting Money in Motion: A New Security Paradigm

At its core, Basefund's approach to transaction security stems from a simple but powerful insight: the most vulnerable moment for funds is when they're in transit. While account security receives significant attention and resources, the actual transfer process—the moment when money moves between accounts—often lacks comparable protection.

The platform addresses this critical gap by creating a comprehensive security layer specifically designed to protect transactions during their most vulnerable phase. Rather than focusing exclusively on securing endpoints or detecting fraud after it occurs, Basefund secures the transaction process itself.

Key Components of the Basefund Security Framework

Account Ownership Verification

The foundation of Basefund's security approach is confirming that funds are going to their intended destination. The platform employs multiple verification methods to ensure account ownership:

✓ Microdeposit verification to confirm account access
✓ Real-time account validation against banking databases
✓ Multi-factor verification processes for new recipients
✓ Ongoing monitoring for account changes

This layered approach virtually eliminates the risk of funds being sent to fraudulent accounts, addressing the most common vector for transaction fraud.

Identity Verification for All Participants

Basefund extends verification beyond just account details to include the identity of all transaction participants. This includes:

✔ Streamlined KYC/KYB processes for all transaction participants
✔ Role-based verification based on transaction sensitivity
✔ Cross-checking of identity information against transaction details
✔ Verification of authority to initiate or approve transactions

By verifying both accounts and identities, Basefund creates a security environment where fraudulent actors struggle to insert themselves into legitimate transaction flows.

Security Without Friction

Perhaps most importantly, Basefund's approach integrates security directly into natural transaction workflows rather than adding it as a separate, disruptive process. By making security an inherent part of the transaction rather than an additional burden, the platform:

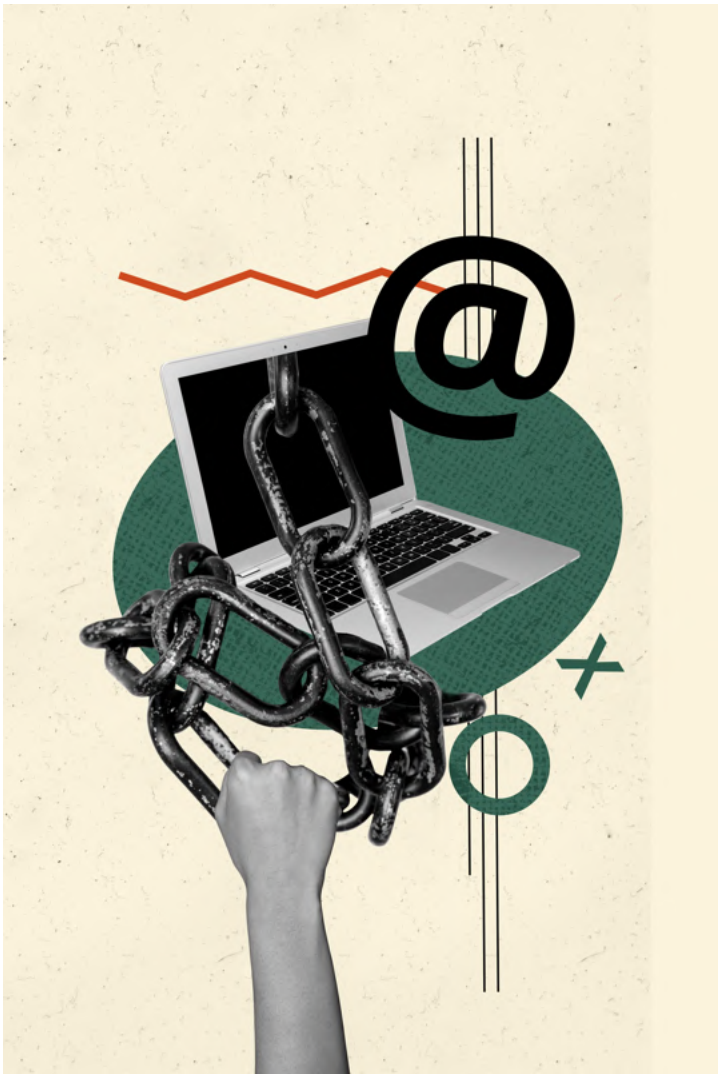
✔ Reduces resistance to security measures
✔ Increases adoption and compliance
✔ Minimizes impact on transaction timing
✔ Maintains strong protection without sacrificing efficiency

Measurable Security Outcomes

Organizations implementing Basefund's approach to transaction security typically experience:

- 100% reduction in successful payment diversion attacks
- 94% decrease in time spent resolving transaction errors
- 73% reduction in payment delays due to security concerns
- 86% improvement in transaction participant satisfaction

These metrics demonstrate that effective security need not come at the expense of efficiency.



The Security Evolution: From Detection to Prevention

Basefund's approach represents an evolution in transaction security thinking—moving from detecting fraud after it occurs to preventing it from succeeding in the first place. This prevention-focused approach delivers substantially better outcomes than traditional detection-based systems, which often identify fraud only after funds have been irretrievably lost.

In a landscape where transaction fraud continues to grow in both frequency and sophistication, Basefund's preventative security framework ensures that financial professionals can conduct business with confidence, knowing that their transactions are protected precisely when they're most vulnerable—when money is in motion.

06 Future Outlook and Recommendations

Emerging Transaction Security Trends

As we look toward the remainder of 2025 and beyond, several clear trends are emerging that will shape the transaction security landscape:

1. The Shift from Point Solutions to Integrated Platforms

The traditional approach of layering multiple security tools is giving way to comprehensive platforms that protect the entire transaction journey. This shift recognizes that security gaps often exist between point solutions, creating vulnerabilities that sophisticated attackers can exploit.

Organizations still relying on fragmented security tools should begin evaluating integrated platforms that cover the full transaction lifecycle, from initiation to settlement. These platforms offer not only better protection but typically improved efficiency and user experience as well.

2. Security Becoming an Enabler, Not a Barrier

The historical tension between security and efficiency is rapidly dissolving as new approaches focus on making secure behaviors the path of least resistance. Rather than adding friction, advanced security systems are being designed to streamline transactions while simultaneously improving protection.

Organizations should evaluate their current security measures through this lens: do they create unnecessary friction, or do they integrate seamlessly into natural workflows? Security systems that create significant operational burdens are increasingly unnecessary and counterproductive.

3. Regulatory Harmonization

Global financial regulators are increasingly aligning their approaches to transaction security, creating more consistent standards across jurisdictions. This harmonization is simplifying compliance for organizations operating internationally while raising the overall security bar.

Organizations with international operations will benefit from security platforms that adapt to these evolving regulatory requirements without requiring significant reconfiguration as standards evolve.

4. The Declining Effectiveness of Training-Only Approaches

While security awareness remains important, the limits of training-centered approaches are becoming increasingly apparent. Human attention is finite, and the sophistication of social engineering continues to grow. Organizations relying primarily on human vigilance face an unsustainable security burden.

The most effective approach combines targeted education with systems designed to catch what humans miss. This balanced strategy recognizes human limitations while still leveraging human intelligence where it's most effective.

Strategic Recommendations for Transaction Security

Based on these emerging trends and the current threat landscape, we recommend financial professionals consider the following strategic priorities:

Implement Comprehensive Protection for Money in Motion

The most critical vulnerability in most organizations' security posture is the gap in protection during funds transfer. While accounts at rest typically have significant security controls, the actual movement of money often lacks comparable protection.

Recommendation: Implement dedicated security systems designed specifically to protect transactions in transit, focusing particularly on external transfers where funds leave organizational control.

Move from Detection to Prevention
Many organizations still focus primarily on detecting fraud after it occurs rather than preventing it from succeeding. While detection remains important, prevention delivers substantially better outcomes—particularly for transaction fraud, where funds are often unrecoverable once transferred.

Recommendation: Shift security resources toward preventative measures that verify account ownership, confirm recipient identity, and validate transaction legitimacy before funds move.

Build Security Into Transaction Design
Rather than adding security as a separate layer, leading organizations are integrating security directly into their transaction workflows. This approach not only improves protection but typically enhances efficiency by eliminating the need for separate security processes.

Recommendation: When designing new payment or transfer processes, incorporate security controls from the beginning rather than adding them later. Consider platforms that offer configurable transaction workflows with embedded security features.

Focus on Account Ownership Verification
The most common transaction fraud vector remains payment diversion to fraudulent accounts. Traditional verification methods like confirming routing and account numbers are insufficient to prevent these attacks.

Recommendation: Implement account ownership verification for all external transfers, particularly for new payment recipients or when banking details change.

Investment Priorities for 2026

As financial professionals develop security budgets for the coming year, we recommend prioritizing investments in:

- Transaction-specific security platforms that protect money in motion
- Account ownership verification systems that confirm funds are going to intended recipients
- Configurable transaction workflows that support different business needs with appropriate security
- Integrated security analytics that identify unusual patterns across all transaction types
- User-friendly security interfaces that encourage adoption and compliance

By focusing investments in these areas, organizations can significantly improve their transaction security posture while simultaneously creating more efficient payment processes.

Preparing for Future Threats

While no one can predict every emerging threat, organizations can develop resilience by building security systems with adaptation in mind. The most future-proof approaches combine:

- Core protection for fundamental transaction risks that remain consistent over time
- Flexible security frameworks that can quickly incorporate new controls as threats evolve
- Access to transaction intelligence networks that provide early warning of emerging threats
- Regular security assessments that identify potential vulnerabilities before attackers exploit them

This balanced approach ensures organizations can adapt to the rapidly changing threat landscape while maintaining strong protection for today's most common attack vectors.

Organizations that approach transaction security with this forward-looking perspective will not only protect themselves against current threats but will be well-positioned to adapt as the security landscape continues to evolve.

07 Conclusion: Building Resilient Transaction Systems

The transaction security landscape of 2025 presents both significant challenges and unprecedented opportunities for financial professionals. As digital transactions continue to increase in both volume and value, the security stakes have never been higher. Yet simultaneously, the tools and approaches available to protect these transactions have never been more powerful.

The Current State: Vulnerability in Transit

Our examination of the current transaction security environment has revealed a critical insight: the most vulnerable moment for funds is when they're in motion. While substantial resources are devoted to securing accounts, the actual transfer process—the movement of money between accounts—often lacks comparable protection.

This vulnerability is compounded by several factors:

- The lack of insurance protection for funds in transit
- The growing sophistication of business email compromise and payment diversion schemes
- The limited effectiveness of human verification alone
- The pressure to complete transactions quickly
- The finality of most digital transfers, which makes recovery of misdirected funds nearly impossible
-

Organizations that recognize and address this fundamental vulnerability position themselves for substantially better security outcomes than those focusing exclusively on endpoint protection or post-fraud detection.

Beyond Technology: A Holistic Approach

While technology plays a crucial role in transaction security, truly resilient systems combine technological controls with appropriate processes and human awareness. The most effective security frameworks integrate:

- Automated verification systems that confirm account ownership
- Identity verification for all transaction participants
- Clearly defined transaction workflows appropriate to different transaction types
- Targeted education that focuses on transaction-specific risks
- Continuous monitoring for unusual patterns or behaviors

This holistic approach recognizes that no single security layer is sufficient in isolation. Only by combining multiple protective elements can organizations create truly resilient transaction systems.

The Path Forward: From Reaction to Prevention

The future of transaction security lies in shifting from reactive to preventative approaches. Rather than focusing primarily on detecting fraud after it occurs, leading organizations are implementing systems designed to prevent fraud from succeeding in the first place.

This preventative mindset delivers several key advantages:

- It protects funds before they leave organizational control
- It creates less operational disruption than recovery efforts
- It reduces both financial and reputational damage
- It decreases the time spent investigating and responding to incidents
- It provides greater peace of mind for all transaction participants

By focusing security efforts on prevention rather than detection, organizations not only improve their protection but typically enhance operational efficiency as well.

Final Thoughts: Trust in Transit

Financial transactions represent trust between parties, with each success strengthening that foundation and each failure weakening it. By protecting money in motion, organizations fulfill a core business responsibility while building trust in our financial system.

Companies that implement security measures protecting transactions at their most vulnerable points will create resilient systems that transaction partners can rely on. As we move through 2025 and beyond, securing money in motion remains critical—those who excel at this challenge will gain competitive advantage through enhanced trust and efficiency.

08 About Basefund

Basefund specializes in protecting money in motion through our comprehensive transaction security platform.

Our mission is to eliminate payment fraud by creating security systems that integrate seamlessly with natural transaction workflows, providing protection without creating additional operational burden. We serve organizations across industries, with particular focus on those managing high-value transactions, complex payment ecosystems, or frequent external transfers.

To learn more about how Basefund can protect your organization's transactions, visit **Basefund.io**