Bottomline

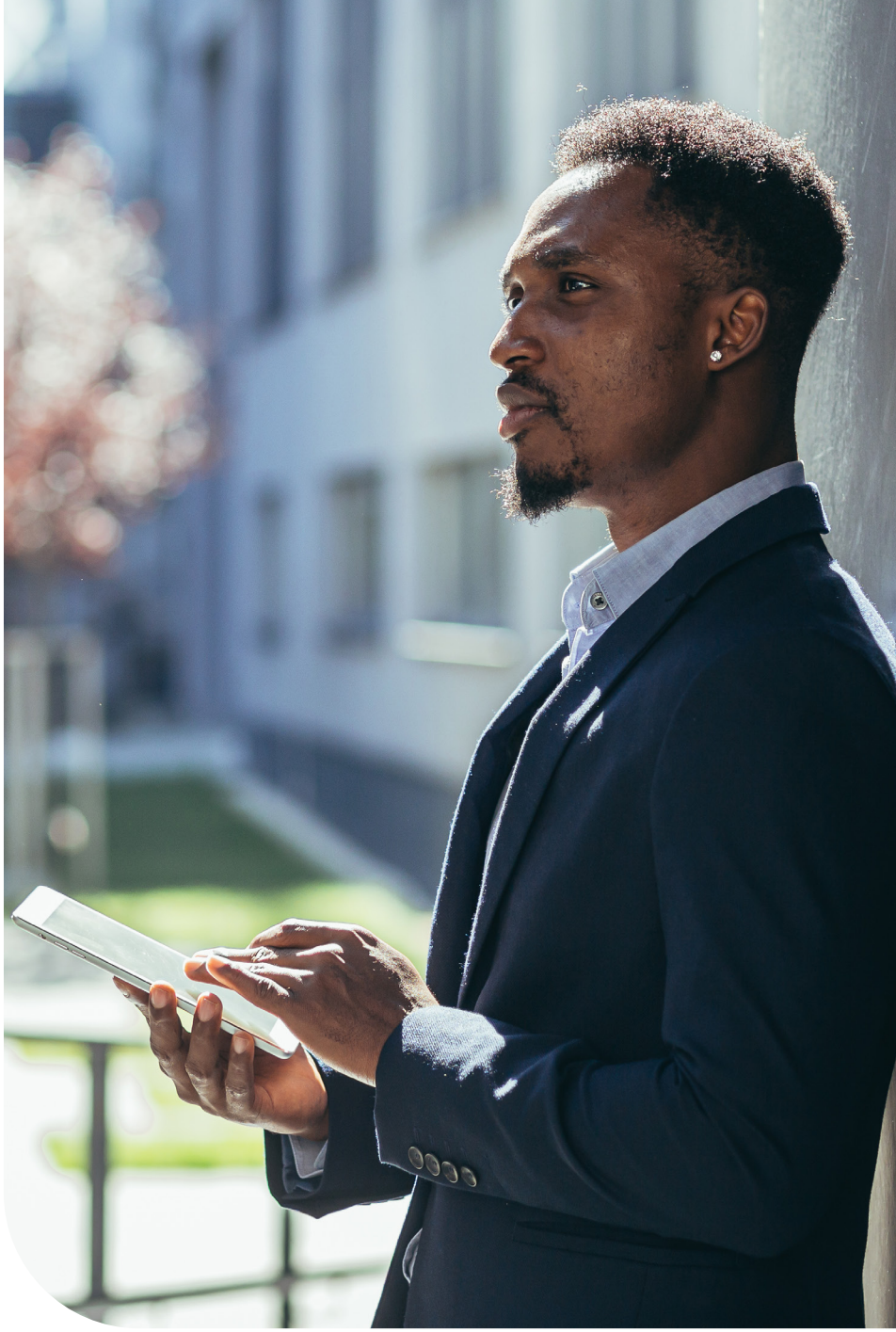
The New Fraud Battlefield

WHY CONTEXT IS KEY

Table of Contents

Today’s fraud is a product of our own innovation. Over the past decade, commercial banking technology has transformed dramatically to support faster payments, new payment rails, and a seamless customer experience. But with that innovation comes more sophisticated bad actors, who leverage the same technologies, specifically AI, to scale their attack strategy.

This puts commercial banking in a challenging spot. The technology that drives its business forward has also expanded its attack surface. Real-time payments move money instantly. ISO 20022 replaces legacy data forms with data-rich messaging standards. Embedded finance brings banking into new environments. With each innovation comes new value, as well as new vulnerabilities.



Here's the Current Landscape:

Percentage of leading banks that use AI to automate manual tasks within payments to detect fraud, process documents, and personalize services.[1]

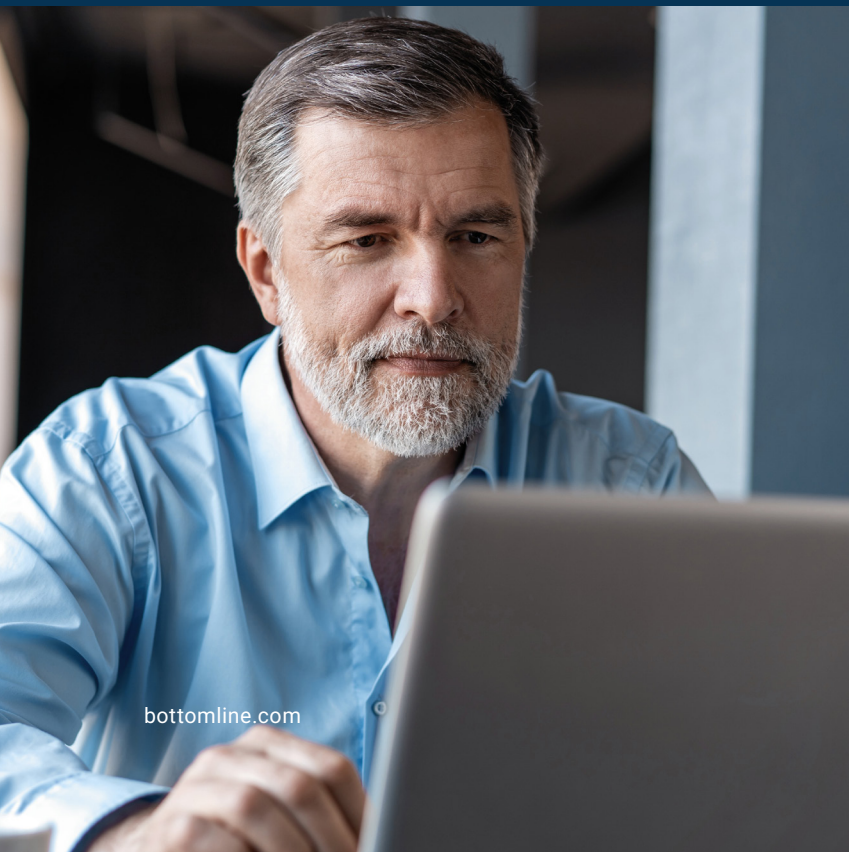
$50B

Global cost of digital payment fraud projected to exceed $50B in 2025.[2]

Nearly eight in ten organizations were targeted by digital payment fraud in the past year.[2]

1 *https://bankingblog.accenture.com/unlocking-gen-ai-commercial-payments*
2 *https://coinlaw.io/digital-payment-fraud-statistics/*

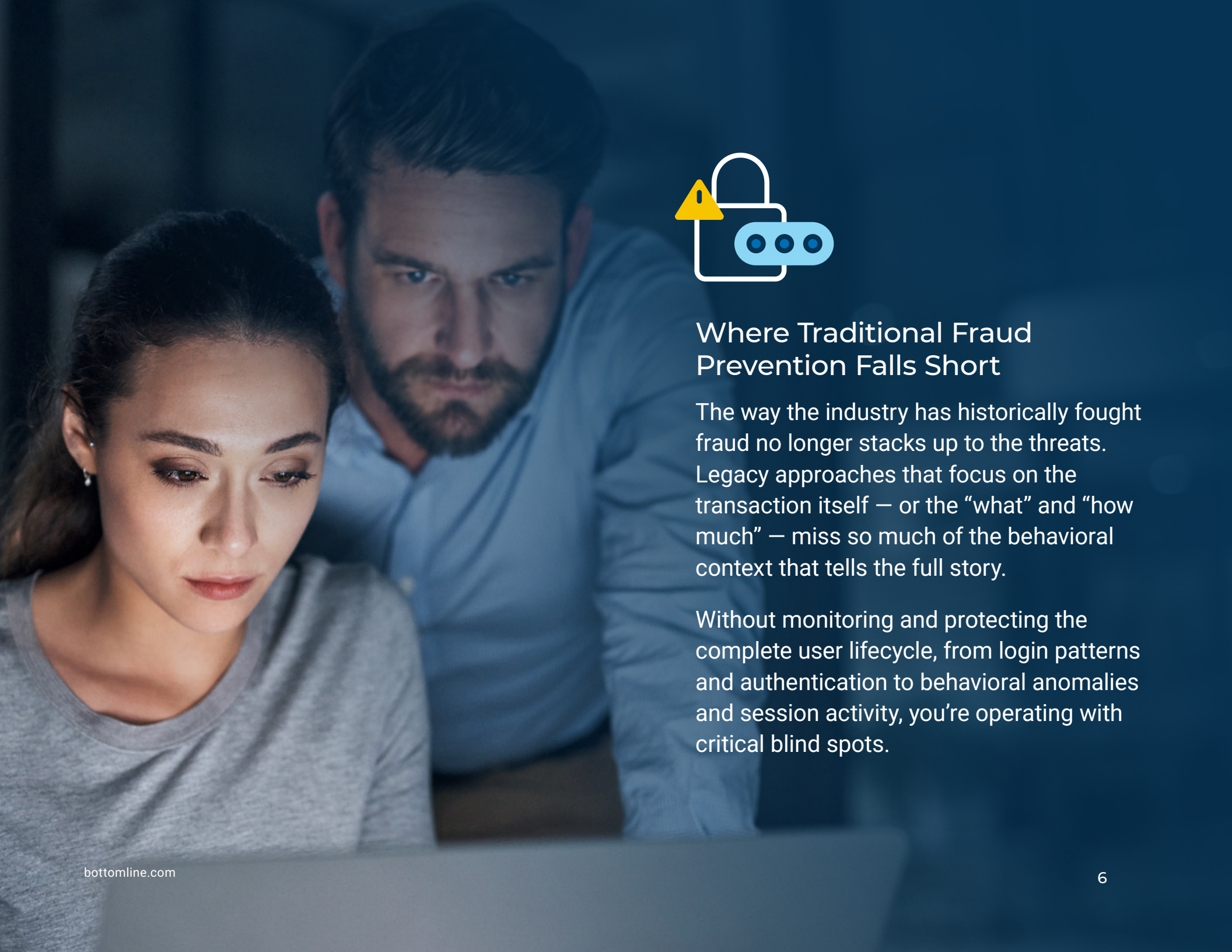
An Accenture report found that only 32% of corporate clients feel that service quality has improved in the last five years.[3]



Keeping your organization thriving in this environment requires resilience, adaptation, and a proactive defense strategy. And those challenges extend beyond technology. An Accenture report found that only 32% of corporate clients feel that service quality has improved in the last five years, and were specifically dissatisfied with their bank's trade finance, liquidity management, and AR/AP services, citing weak fraud controls and difficulty using payment solutions.[3]

In an era where a strong customer experience is a critical competitive advantage, banks can't afford to compromise. The question isn't whether or not to innovate, but how to do so without expanding your vulnerability. In this eBook, we'll dive into the most critical fraud threats targeting modern payment systems, the gaps in traditional defense, and how to build a layered fraud prevention strategy that protects every part of the payment lifecycle.

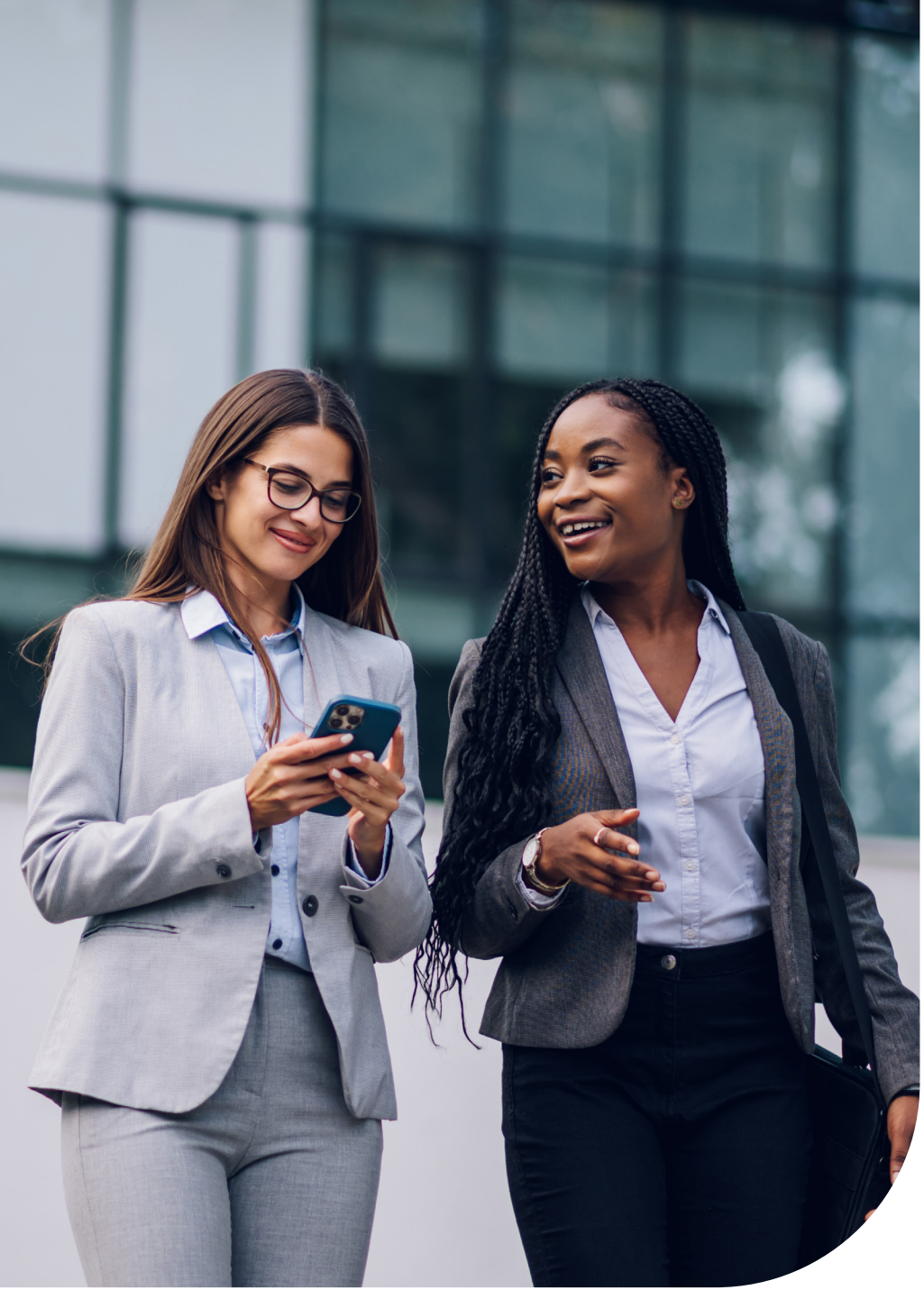
3 https://bankingblog.accenture.com/unlocking-gen-ai-commercial-payments



Where Traditional Fraud Prevention Falls Short

The way the industry has historically fought fraud no longer stacks up to the threats. Legacy approaches that focus on the transaction itself — or the “what” and “how much” — miss so much of the behavioral context that tells the full story.

Without monitoring and protecting the complete user lifecycle, from login patterns and authentication to behavioral anomalies and session activity, you’re operating with critical blind spots.



Mind Your Gaps to Build Resilience

Fraud prevention used to be measured by how well you protected the core banking system. Unfortunately, that definition no longer applies.

Today, operational resilience means protecting the entire payment ecosystem through every channel and touchpoint in the user journey.

Banks must detect anomalies in real time, not hours or days later. Part of this includes knowing what is normal behavior, and what isn't — and where investigators should focus their energy.

Modern payment ecosystems introduce complexity at every layer. Here's where those gaps typically appear:

At vendor onboarding…

- Lack of robust identity verification
- Insufficient validation of banking details before first payment
- No continuous monitoring after initial approval

At authentication…

- Static credentials that can be easily compromised through phishing
- Inadequate multi-factor authentication across payment channels
- Missing behavioral analysis to detect account takeover attempts

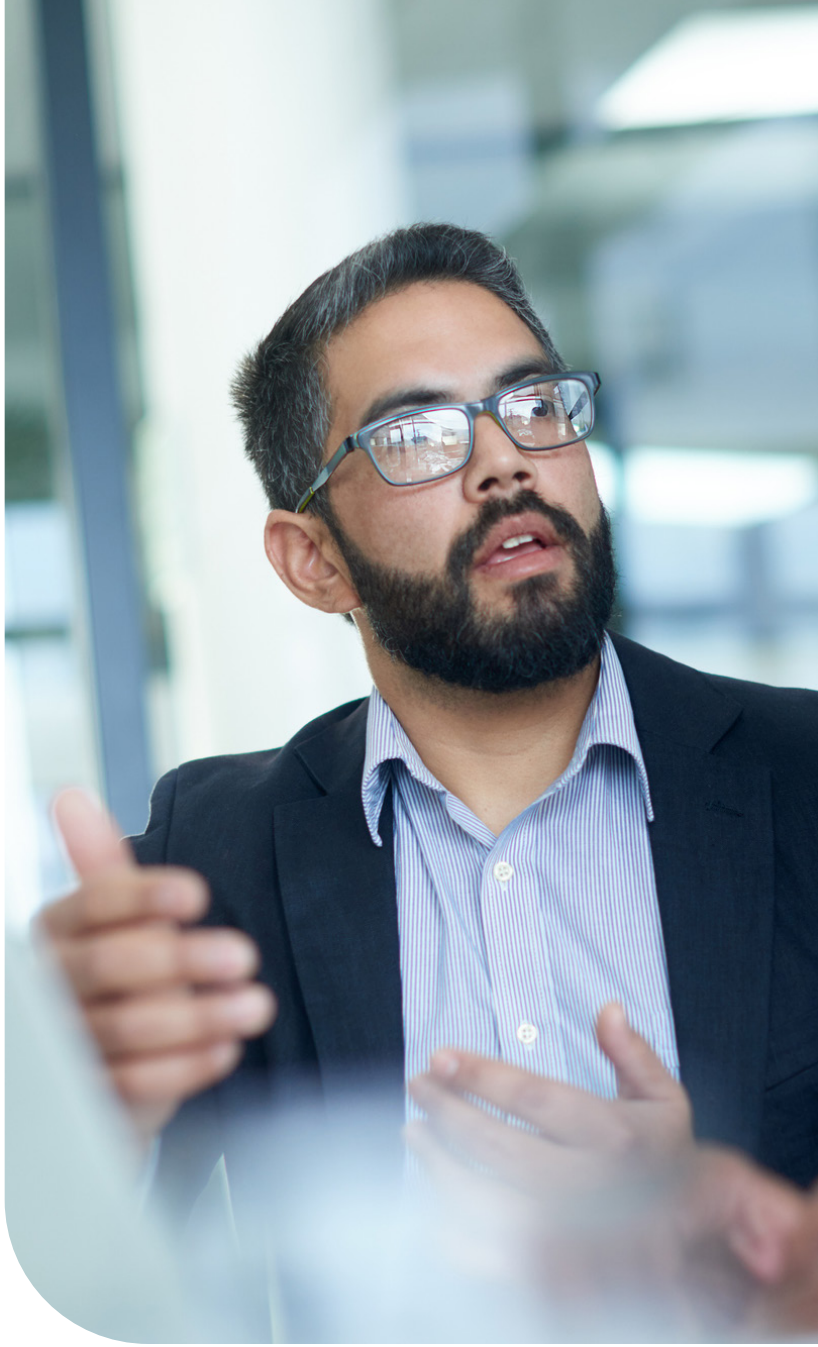
In transaction patterns…

- High-value, low-frequency transactions that deviate from historical norms
- New payment destinations that didn't follow proper verification protocols
- Off-hours payment initiation that breaks established patterns

Banks must detect anomalies in real time, not hours or days later.

Each new innovation in the payment landscape brings new attack vectors. Because real-time payments are instant and irrevocable, they leave little to no time for traditional review. Extending banking capabilities through embedded finance into third-party platforms multiplies touchpoints requiring protection. When it comes to protecting cross-border payments, standard updates around ISO 20022 will help create a universal language for payments data so markets and institutions can communicate seamlessly around the globe.

To balance innovation with the new face of fraud, you need to know what you're up against. Today's fraud landscape is dominated by several key attack vectors, each weaponizing AI in their own way to make it even harder to distinguish legitimate from suspicious behavior.



Problem: Social Engineering

What it is

Social engineering involves sophisticated psychological manipulation, often using AI to generate convincing deepfakes, documents, and communications. Fraudsters also use AI to customize campaigns to each target, studying their communication patterns, relationships, and vulnerabilities for maximum impact. Attackers use tactics centered around creating urgency, trust, and fear, all while taking advantage of remote work and digital engagement patterns.

Why it matters

Phishing is the most common social engineering tactic, accounting for 91% of social engineering attacks in 2025, but the landscape is changing fast.[4] Attackers are using AI at scale to build their deeply personal and targeted campaigns, which often include studying their target and their communication patterns, relationships, and potential vulnerabilities. Though AI-built emails accounted for almost 82% of campaigns in 2025, other tactics like vishing (voice phishing), smishing (SMS or text phishing), or quishing (QR code phishing) are on the rise. including deepfake document or video creation, or voice spoofing.[5] [6]

4 https://www.knowbe4.com/resources/reports/phishing-by-industry-benchmarking-report
5 https://guardz.com/blog/33-phishing-statistics-in-2025-every-msp-should-know-about/
6 https://deepstrike.io/blog/Phishing-Statistics-2025

How Bottomline defends against it

Bottomline connects and correlates analytics across the entire payment journey, from user login and authentication to session activity. This offers users a view into behavioral inconsistencies that can signal social engineering attacks. Bottomline ingests and analyzes all payment activity to build a comprehensive picture of what's normal, and what's not.

The platform supports real-time user challenges and payment interdiction when anomalies are detected. With advanced tuning, you can group customers by segment and forecast the impact of model updates before deployment. With the Record & Replay feature, investigators can visualize actual user behavior and access cross-platform analytics to reduce investigation time and connect patterns across what seem to be routine requests on the surface.

The takeaway:

A sophisticated impersonation fails only when the behavioral inconsistencies add up to signal fraud. A routine payment request that deviates from historical approval patterns, arrives through new communication channels, or creates fake urgency that doesn't match past behavior, should all send up red flags.

Account Takeover (ATO)

What it is

To commit account takeover, attackers use common forms of social engineering, such as phishing, to steal credentials and gain unauthorized access to legitimate user accounts. Then, they “takeover” the account, operating from within to initiate fraudulent payments, change payment destination details, or steal sensitive information.

Why it matters

By 2026, merchants expect to lose $91 billion to account takeover fraud.[7] And with more than 83% of corporations experiencing at least one account takeover attack in the past 12 months, this form of fraud is surging.[8] The threat is compounded by the rise of cross-border payment attacks, as instant payments and ISO 20022 standards introduce new complexity into banking that creates additional opportunities for credential theft. Like the many forms of social engineering, AI has transformed the methods and scale at which attackers can strike. Fraudsters can now create eerily convincing deepfakes and fake identity documents that slip past traditional verification methods.

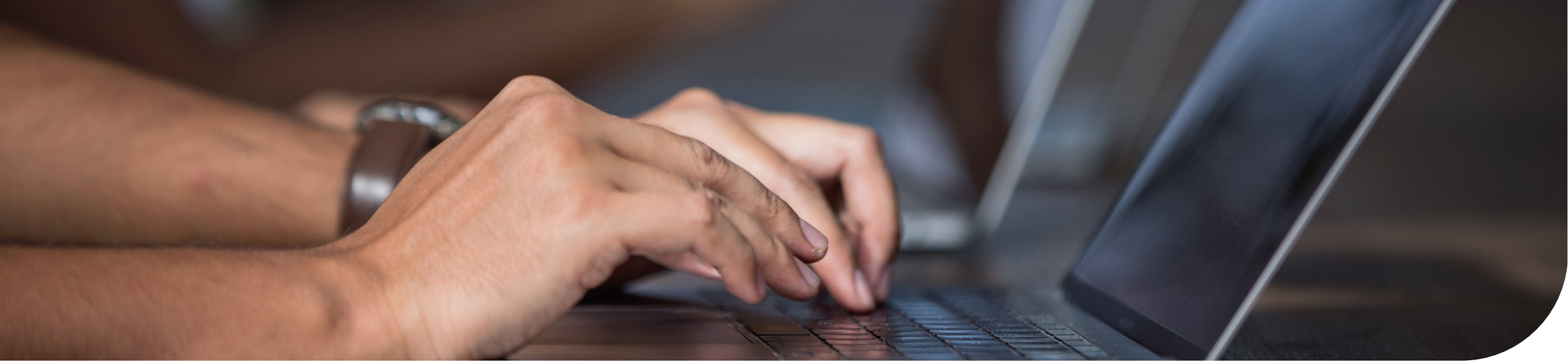
7 https://www.juniperresearch.com/press/losses-online-payment-fraud-exceed-362-billion/#
8 https://abnormal.ai/resources/state-of-cloud-account-takeover-attacks

How Bottomline defends against it

Defeating account takeover requires knowing exactly when it starts. This means fraud prevention that begins at onboarding and monitors user login and authentication patterns to establish a baseline of activity. This includes following typical devices, geolocations, login times, and usual session behavior. Then when something is off, from an unrecognized device to an unusual geolocation or login time, the platform can trigger real-time user challenges. Device fingerprinting flags suspicious endpoints, while behavioral analytics monitor session activity. With advanced tuning, you can set risk thresholds by customer segment, so high-risk scenarios encounter additional friction.

The takeaway:

An unusual login is often the first sign of trouble. When someone logs into a corporate bank account from a new device in an unfamiliar location and immediately attempts to wire a large transfer, account takeover could be at play. Behavioral analysis flags suspicious activity that transaction monitoring alone would miss.



Business Email Compromise (BEC)

What it is

Another form of social engineering, business email compromise (BEC) occurs when attackers impersonate executives, vendors, or business partners through spoofed emails, spearphishing campaigns, or vendor fraud schemes. Often called CEO fraud, these attacks exploit trust relationships to authorize fraudulent payments.

Why it matters

According to the FBI IC3 2024 Report, BEC losses exceeded more than $2.7 billion globally in 2024 — a more than 1,000% increase since 2015.[9] [10] But the threat goes beyond dollars — the sophistication has evolved dramatically. Today's scam emails aren't nearly as obvious as they were even a few years ago, thanks to AI tools that create convincing communications that look and sound like a legitimate request. The attacks are also more strategic. Pretexting, or the setup behind the scam that creates a false urgent situation to justify a request for payment or information, has become standard setup behind successful BEC campaigns. Bad actors often research organizational structures, study communication styles, and time their attacks to exploit busy periods or staff transitions, making the deception extremely difficult to spot.

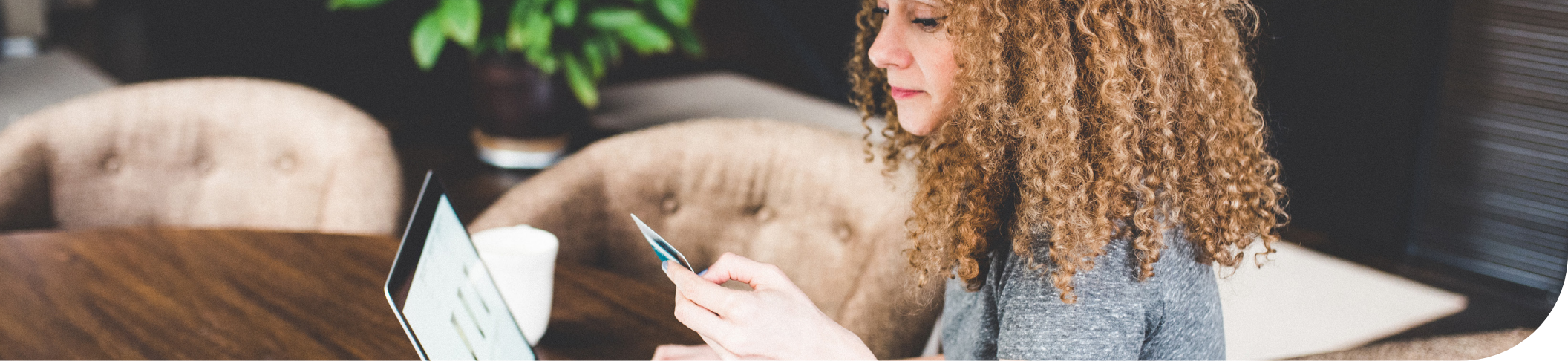
9 *https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf*
10 *https://abnormal.ai/blog/2024-fbi-ic3-report*

How Bottomline defends against it

BEC attacks often succeed by mimicking legitimate business processes. To stop them, we must analyze payment requests in the context of normal approval workflows and historical patterns. Bottomline ingests and analyzes all payment activity to create a baseline of typical user and relationship behavior. When a payment request deviates from those patterns, such as a wire to a new vendor or an unusually large invoice payment, the platform flags it for review. With specific risk thresholds set for certain activities, such as a new payee or automatically holding suspicious payments, investigators can slow the process down for a closer look. By leveraging Bottomline's consortium data built on trillions of transactions executed globally, the system can also identify when a new fraud pattern emerges at other institutions and apply those learnings to protect your organization.

The takeaway:

The most convincing BEC scams exploit trust, such as an email from your CEO that looks and sounds like them. But when behavioral monitoring reveals that the request bypassed the usual approval workflow and targets a new vendor, it's a whole different story. Context is the difference between losing millions and catching fraud before the funds transfer.



Digital Payments Fraud

What it is

Digital payments fraud includes attacks that target digital payment channels including credit cards, ACH, real-time payments, and eCommerce platforms. The methods can range from credential theft to sophisticated social engineering rings. Customers expect multiple payment channels, including mobile banking, digital wallets, or instant payments, leading to many entry points that require protection.

Why it matters

While each digital payment rail operates with different speeds, rules, and recovery mechanisms, fraud detection must work seamlessly across all of them. Digital payment fraud is projected to exceed $50 billion globally in 2025, with 79% of organizations already targeted in the past year.[11] But the true cost goes beyond immediate financial losses. Reputation and brand damage and brand can drive customers to competitors, creating long-term revenue impact. AI-driven fraud dramatically increases success rates, particularly for real-time and cross-border attacks where traditional detection methods struggle to keep pace. And with each incident, regulatory scrutiny intensifies, bringing potential fines and restrictions.

11 https://coinlaw.io/digital-payment-fraud-statistics/

How Bottomline defends against it

Stopping digital payments fraud requires protection across every channel, at the same time. Because Bottomline ingests and analyzes all payment activity, you gain comprehensive visibility, regardless of the payment rail. The platform connects and correlates data across the payment journey in real time, including transactional data, behavioral patterns, and device signals, to get a complete view of the payment journey. By using this cross-channel intelligence, you can spot patterns in real time that single-channel monitoring would miss, such as a fraudster testing small amounts via ACH before attempting a large wire transfer. Fraud detection that can keep pace with real-time, high-value transactions — all without creating friction for legitimate payments — is critical to preventing digital payments fraud.

The takeaway:

In the world of instant payments, you don't get a second chance. When a legitimate-looking wire request shows red flags, such as a new device, unusual timing, or unfamiliar beneficiary, real-time interdiction is critical to stopping massive losses.

Authorized Push Payment Fraud

What it is

With authorized push payment (APP) fraud, victims are tricked by bad actors through impersonation or manipulation into voluntarily transferring money to fraudulent accounts. These victims believe that they're making legitimate payments, when in fact they've been caught up in investment scams, invoice fraud, romance scams, and impersonation of businesses or government authorities. The challenging part of preventing APP fraud is that the victim themselves authorizes the payment. For commercial banks, this can come in the form of fake vendor invoices, or impersonating a supplier or executive.

Why it matters

Traditional controls that look for unauthorized access can miss APP fraud entirely, because there is no illegitimate account access. The challenge is compounded by the nature of real-time transfers; once the money is sent, recovering it becomes extremely difficult, if not impossible. And the stakes are high: Deloitte estimates losses in the U.S. from APP fraud to reach $15 billion by 2028.[12] Legacy risk controls, designed for slower payment systems with built-in review periods, simply aren't effective against rapidly evolving APP scams. So if the user authorizes the payment, who is liable? Traditionally, the consumer is on the hook for the funds. However, liability has begun shifting in the U.S. toward banks, as means of putting pressure on them to step up their fraud controls. Nacha, which oversees the ACH network, is implementing new rules that will require all non-consumer ACH participants to monitor for suspected fraud by mid-2026.[13]

12 https://www.deloitte.com/us/en/insights/industry/financial-services/authorized-push-payment-fraud.html
13 https://www.nacha.org/news/new-nacha-rules-new-fraud-compliance-responsibilities-all-organizations-sending-ach-payments

How Bottomline defends against it

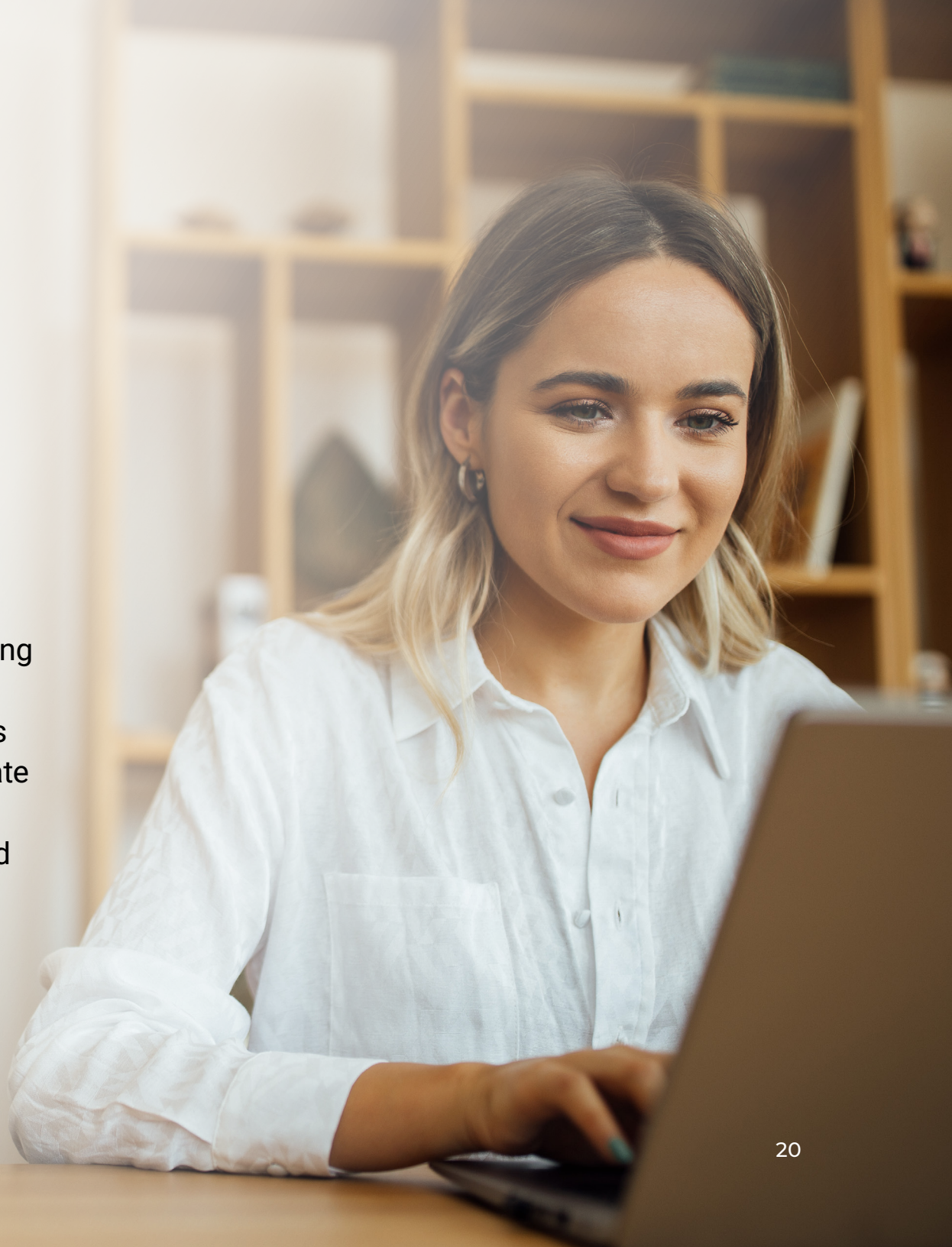
APP fraud requires a different defense, because the transaction itself is legitimate. Bottomline can help solve this by analyzing the payment itself in the context of behavioral patterns and relationships. Because the platform ingests and analyzes all payment activity to establish a normal baseline, changes from the norm are immediately flagged. With real-time payment interdiction, suspicious transactions can be held at the point of initiation. With powerful consortium data across trillions of global transactions, APP fraud patterns begin to emerge.

The takeaway:

Though APP fraud can hide behind legitimate credentials, it often can't account for stark behavioral red flags, such as new payee accounts in combination with large transfers. Without the context of established behavior, the authorization may seem legitimate.

A Layered Fraud Prevention Approach

The modern fraud landscape requires a radically different approach than what worked in the past. Transaction-only analysis misses the behavioral context where early warning signs appear, signaling fraud like account takeover or business email compromise. Siloed point solutions that monitor individual channels can create dangerous gaps in fraud prevention. Put simply, the legacy way of preventing fraud is entirely too slow for today's world.

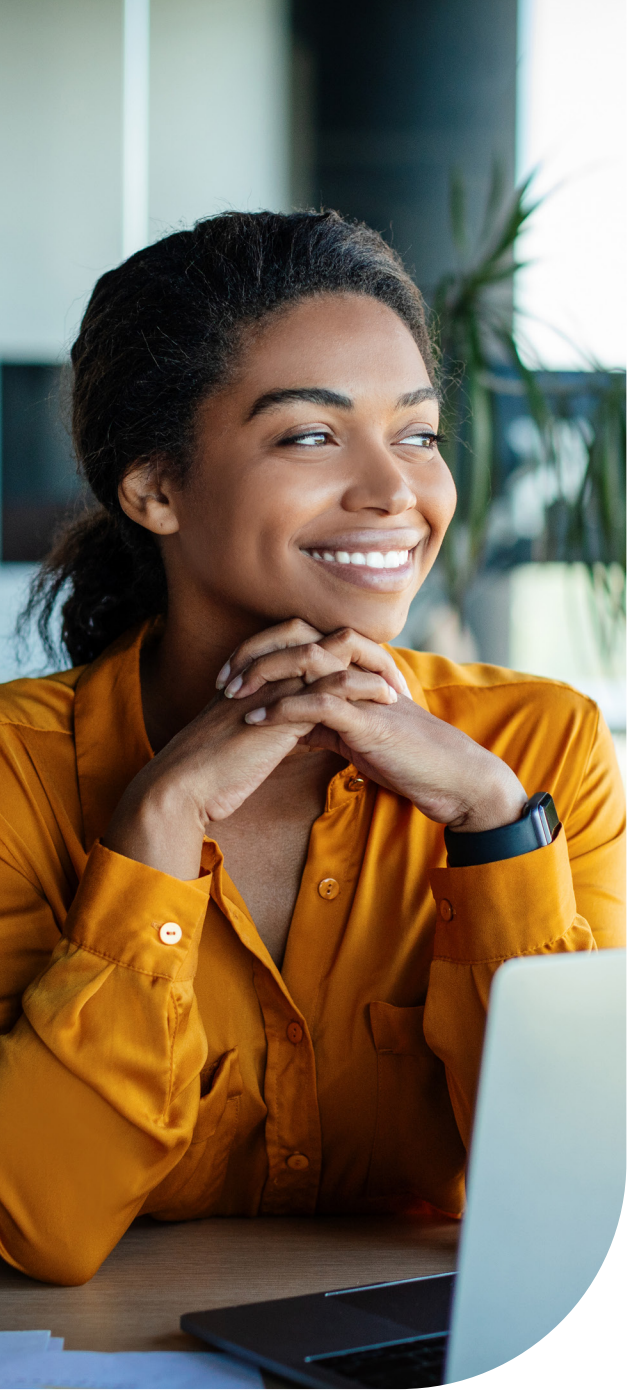


The legacy way of preventing fraud is entirely too slow for today's world.

Effective fraud prevention requires:

- **Real-time, integrated monitoring** across every layer of the user journey, including authentication, session activity, behavioral patterns, and transaction execution. Anomalies at the login stage can prevent fraud before a transaction is ever initiated.
- **Consortium intelligence** that shares attack patterns across institutions. When a tactic appears at one bank, others gain immediate insight.
- **A risk-based approach** that balances security with customer experience. Not every transaction will require the same scrutiny, and adaptive controls can apply friction where necessary.
- **Empowered investigators** who are equipped with enriched data, cross-platform analytics, and visualization tools that dramatically reduce investigation time. When suspicious activity is flagged, analysts need the complete picture to make informed decisions quickly.
- **Continuous improvement** through machine learning that evolves with the threat landscape. Static rules fail as attackers adapt, but models that learn from new patterns can stay ahead of emerging tactics.

True fraud prevention monitors the digital banking channel itself, where users authenticate, navigate, and ultimately initiate payments.



Building Your Defense with Bottomline

The fraud landscape has fundamentally transformed. Attackers have industrialized their operations, weaponizing AI to scale attacks with shocking sophistication. Meanwhile, banks navigate mounting regulatory pressure, customer demands for seamless experiences, and the operational challenge of protecting an ever expanding attack surface.

Traditional approaches focused on transaction monitoring can leave you blind to the behavioral signals that quietly precede fraud. Without visibility into authentication patterns, session activity, and user behavior, you're making critical security decisions with incomplete information. And with faster payments and real-time settlement, the window between attack initiation and financial loss has collapsed to seconds.

The commercial banking clients you serve expect both security and seamless experience. They demand support for multiple payment channels, instant settlement options, and frictionless transactions. The payment innovations they expect — real-time rails, cross-border capabilities, and embedded finance — aren't going away. The challenge is securing them without sacrificing the customer experience.

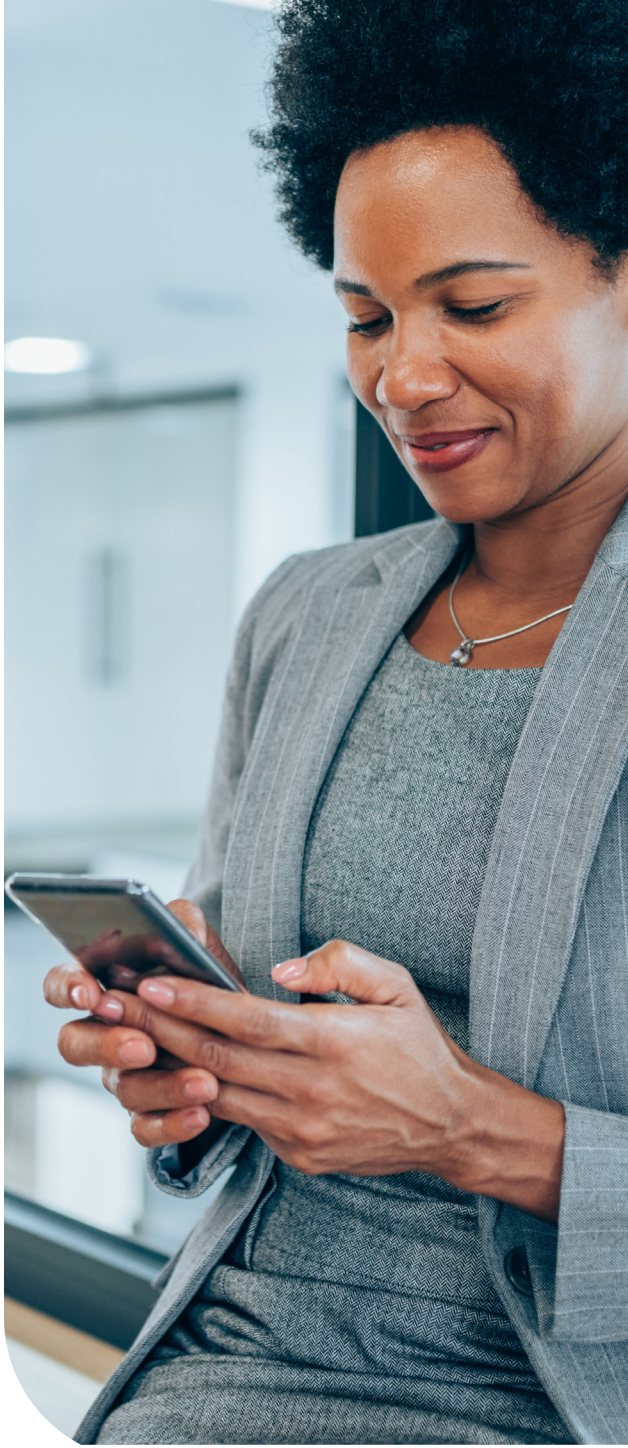
Bottomline's risk solutions deliver the modern architecture commercial banks need: extensible platforms that deploy rapidly, integrate seamlessly across your payment ecosystem, and evolve as threats change. By ingesting and analyzing all payment activity across the entire user journey, connecting behavioral intelligence with transaction data, and leveraging consortium insights from trillions of global transactions, Bottomline helps you detect fraud before it becomes a loss, without creating friction for legitimate customers.

The fraud tactics outlined in this playbook — social engineering, account takeover, business email compromise, digital payments fraud, and authorized push payment fraud — will continue evolving. Your defense strategy must do the same.

Ready to strengthen your fraud defenses?

Learn more about building a modern, layered fraud prevention strategy that protects every stage of the payment lifecycle.

Learn More



Bottomline

REV US010826LM