Bottomline®

Under Attack: The New Reality of Commercial Fraud Prevention

Protecting the Core Banking System isn't Enough

Imagine detectives trying to solve a crime by only looking at the getaway car. They might know that something happened, but not who did it, why, or how they pulled it off. That's exactly how many banks at the commercial level fight fraud: focused solely on the transaction, or the "what" or "how much," while missing the authentication (who), the behavioral context (why), and the session data (when). Without these pieces, you're left making high-stakes decisions with incomplete information. **That's not risk management — that's guesswork.**

THIS IS WHAT YOU'RE UP AGAINST:

78% Nearly eight in ten organizations were hit by payments fraud attempts in 2024.[1]

70% Enterprise banks reported the largest spike in fraud attempts, with nearly 70% seeing a significant increase in fraud over the past year.[2]

$8.5B Reported losses from business email compromise (BEC) from 2022-2024.[3]

And the losses go beyond dollars — reputational damage and customer attrition can cost even more in the long run. Protecting your banking system comes down to how you respond to pressure. Read on as we dive into what this internal and external pressure looks like, the cost of getting it wrong, and how to build and execute a strong fraud prevention approach.

1. https://www.financialprofessionals.org/training-resources/resources/survey-research-economic-data/details/payments-fraud
2. https://www.alloy.com/reports/fraud-report-2025
3. https://www.nacha.org/news/fbis-ic3-finds-almost-85-billion-lost-business-email-compromise-last-three-years

External Pressure: A Changing Landscape

Starting on the outside, fraud and risk teams within banks are getting hit from all sides. This external pressure can look like:

Evolving Fraud Threats

While most have heard about deepfakes, account takeover, and business email compromise, few have figured out exactly how to stop them. With digital fraud projected to top $50 billion in 2025, the industry is struggling to keep pace with these threats.[4] This disconnect often stems from siloed operations, where security and customer experience teams aren't aligned and fraud prevention is treated as a "back office" problem, instead of an organization-wide priority.[5]

To make matters worse, fraudsters have evolved their tactics, now targeting corporate and commercial customers with deeper pockets. And while the fraud methods may be familiar, the stakes are much higher.

Protecting both your institution and its customers has never been more challenging. According to the Association for Finance Professionals' 2025 Payments Fraud and Control Survey, 80% of organizations experienced payments fraud attempts in 2024.[6]

With digital fraud projected to top **$50 billion in 2025,** the industry is struggling to keep pace with these threats.[4]

Weaponizing Fraud at Scale with AI

While 91% of banks report using AI for fraud detection, bad actors are using it with equal success.[7] Thanks to the prevalence of inexpensive AI tools, fraud has become industrialized and scalable, helping criminals carry out nearly flawless phishing and scam attempts.

Deepfakes represent one of the most alarming applications. The technology is being used for everything from bypassing facial biometric gates to creating nearly authentic identity documents. One report showed an 1,100% increase in deepfake attempts in the first quarter of 2025 alone.[8]

Business Email Compromise (BEC)

was the primary payments fraud attack vector, cited by 63% of respondents in the 2025 Payments Fraud and Control Survey. Gone are the days of obvious scam emails that are riddled with poor grammar and typos. By using AI, bad actors can generate highly believable emails that look and feel like the real thing. One common method is by using "pretexting," or creating a false, urgent situation as a pretext to asking for a funds transfer or sharing confidential information.[9] According to Verizon's 2024 Data Breach. Investigation Report, the use of pretexting is more likely than phishing and continues to be the leading cause of cybersecurity incidents at 73% of breaches.[10]

Account takeover (ATO) attacks are on the rise with similar persistence.

A 2024 report revealed that **more than...**

of corporations experienced at least one account takeover attack in the past 12 months,[11]

with

experiencing an ATO attempt every week.[11]

Accounting for not only the volume but the ***sophistication*** of these attacks can leave banks floundering, unsure where to look first and stuck using static, rule-based methods for fraud detection.

Regulatory Rules are Constantly in Flux

The regulatory landscape is shifting faster than ever. According to a recent Bottomline survey, 32% of respondents listed hitting compliance and regulatory deadlines as a top priority over the next 12 months. And for good reason — Fall 2025 brings deadlines for critical mandates such as Instant Credit Transfers (SEPA Inst) and Verification of Payee (VoP), and ISO 20022 migration.

Meeting these requirements will require modern infrastructure and enhanced data capabilities, not to mention regulatory defensibility for all of the above.[12] And with global enforcement totals surpassing $19 billion in 2024, your fraud solutions must be audit-ready and flexible. Unfortunately, there's no margin for error.

4. https://coinlaw.io/digital-payment-fraud-statistics/
5. https://www.bankingexchange.com/news-feed/item/10382-in-the-age-of-ai-banks-must-redefine-fraud-prevention
6. https://www.financialprofessionals.org/training-resources/resources/survey-research-economic-data/details/payments-fraud
7. https://www.elastic.co/blog/financial-services-ai-fraud-detection
8. https://sumsub.com/newsroom/synthetic-identity-document-fraud-surges-300-in-the-u-s-sumsub-warns-e-commerce-healthtech-and-fintech-at-risk/
9. https://www.darktrace.com/blog/business-email-compromise-bec-in-the-age-of-ai
10. https://www.verizon.com/business/resources/reports/dbir./
11. https://abnormal.ai/resources/state-of-cloud-account-takeover-attacks
12. https://d15fjz85703yz4.cloudfront.net/4617/4672/6014/Competitive-Banking-Report-Infographic-5-040225.pdf
13. https://www.bottomline.com/resources/blog/frauds-fast-lane-pwc-new-rules-commercial-banking-fraud-and-risk

The Cost of Getting it **Wrong:**

U.S. businesses reported **losing the equivalent of 9.8% of their revenue** to fraud over the past year.[13]

Unresolved incidents trigger regulatory scrutiny, with millions in potential fines and operational expenses.

A major public fraud incident can **break trust and drive commercial clients to competitors,** leading to long-term losses in customer relationships.

Internal Pressure: Doing More with Less

When it comes to pressure from inside their institutions, the situation isn't much better. While banks are responsible for combating this evolving threat landscape, they're being asked to do so with tighter budgets and mounting pressure to demonstrate fast ROI from their fraud and compliance investments.

The customer experience must be front and center. Fraud and risk teams face a constant balancing act: apply strong enough controls to stop fraud, but not so much friction that legitimate customers are disrupted. Organizations expect the services offered by their commercial bank to be accessible, efficient, reliable, and secure.

"You've got this constant tension between providing the **best product** and **possible customer experience** at the **best margin** for your customer, while also protecting them effectively. That's not an easy decision, and it is dynamic. **It's constantly shifting**."

Alex West, PwC Partner, Banking and Payments[13]

Those same customers also demand seamless support of a range of payment channels like real-time payments, ACH, and wire. Every new payment channel only increases your attack surface, and teams must detect fraud faster in real time, without impacting the user experience. At the commercial banking level, there's very little room for error.

32% of surveyed banks plan to make adding new payment rails a **priority** in the next 12 months.[14]

Meanwhile, running a department of fraud investigators means staying ahead of burnout and ensuring analysts see the true value of their work. As a significant cost center, operating this function efficiently is critical yet increasingly challenging.

The Cost of Getting it **Wrong:**

With a staff turnover rate of **nearly 20%**, the banking and finance sector is often hit the hardest with burnout due to alert fatigue and constantly being in firefighting mode.[15]

Tight budgets create a challenging balance. **56%** of fraud and risk teams report their teams have not grown headcount, while attack attempts have risen more than **30%.** Automation can help counteract this pressure, but it's not a complete solution.[16]

84% of consumers would switch banks if that institution were linked to financial crime, and **87%** would actively warn family and friends against using that institution.[17]

14. Bottomline: Fourth Annual Global Report: The Future of Competitive Advantage in Banking & Payments
15. https://gethppy.com/employee-turnover/the-millennial-turnover-problem-in-the-financial-services-industry
16. https://www.alloy.com/blog/2025-financial-fraud-statistics
17. https://financialit.net/news/banking/84-consumers-would-switch-banks-over-financial-crime-links-thetaray-report-finds

Your Blind Spots are Costing You

Taking a legacy approach to monitoring your core banking system means you're only getting half the story: transaction information, but without the context of behavior, login patterns, and session activity data.

Bad actors aren't working in silos, targeting just one area of your business, so why are fraud and risk teams working that way?

What if you could see an attack as it builds at the behavior level, **before** the fraudulent transaction even happens?

It’s Time to Take an Integrated, Multi-Layered Fraud Approach

In fraud prevention and detection, context is key. Without monitoring all the layers of the user lifecycle, from login patterns and usual behavior to the transaction level, you’re missing out on critical pieces of the story.

An integrated flow should look like:

DETECT: Continuously build profiles to detect anomalies and suspicious behavior, such as the usual payors and payees (the who), the payment channels and amount frequency (the what), the standard geolocation of the device (the where), what time of day and month transactions usually occur (the when) and finally the why: recurring payment or vendor payments.

PREVENT: Build a risk score to alert on high-risk activity such as a new payee, an off-hour payment initiation, or a new location login.

RESOLVE: Investigate the risk score to either block or release the transaction

Because this approach blends all the best parts of fraud fighting — human-in-the-loop decisions, the power of consortium data, and a layered approach — teams can assess risk in real time and actively prevent payment fraud. It’s a proactive approach to risk management that removes unnecessary complexity while preserving the user experience.

The benefits extend beyond fraud prevention. Investigations become simpler and more productive, reducing analyst burnout. Integrating robust fraud monitoring into compliance strategies helps reduce risk, ensure readiness for upcoming mandates, and improve operational efficiency.

With innovations in real-time payments, cross-border capabilities, and ISO 20022 messaging reshaping the industry, commercial banks need infrastructure that can keep pace. **The answer isn’t bolting more point solutions onto legacy systems — it’s adopting an integrated approach that protects every layer of the customer journey.**

Full-Spectrum Fraud Prevention with Payments Fraud Defense

Many banks already have fraud detection solutions at various points in the payment lifecycle — perhaps at accounts payable or at the payment rail level. While these are valuable, they only tell part of the story. True protection requires a multi-layered approach that monitors fraud within the digital banking channel itself.

Commercial banking fraud requires a fundamentally different approach than retail. With high-value, low-volume transactions and multiple user touchpoints per account, commercial customers need sophisticated monitoring without the friction that drives them to competitors.

It's not enough to rely solely on fraud detection at the core banking system. Those solutions are limited to transaction data, or the dollar amounts, but they don't capture the behavior, login patterns, or session activity that can signal fraud before a transaction even occurs.

An integrated, multi-layered approach to fraud starts with Bottomline Payments Fraud Defense.

A next-generation monitoring solution, Payments Fraud Defense is built for rapid deployment with an extensible, modernized architecture that delivers stronger security and enhanced performance—**without the complexity of traditional enterprise implementations.**

THE POWER OF CONSORTIUM

Out-of-the-box, the solution is rich with learnings from banks across the Bottomline network that are using Payments Fraud Defense to fight fraud. This means knowing when patterns seen at one bank pop up at another.

VISUALIZE USER BEHAVIOR IN REAL TIME

With Record & Replay, real-time, non-invasive monitoring allows you to visualize user behavior and access powerful cross-platform analytics. This is where the complete picture of risk comes together, allowing you to enrich monitored data with additional insights and dramatically reduce investigation time.

CUSTOMIZE FOR YOUR NEEDS

Prevent fraud loss by automatically putting transactions on hold so suspicious activity can be examined in the case management center. Investigators get a full understanding of risk, allowing them to connect the dots between users, accounts, transactions, and data. Once the investigation is complete and funds are verified, analysts can release funds or block them if determined fraudulent.

30%

fewer false positives using BTune

TAILOR AND TUNE CUSTOMER SEGMENTS

Using BTune, partner with Bottomline's fraud experts to carefully tune your customer segments and fraud analytics to reduce risk. Tailored to your risk tolerance, empower your investigators with only the highest quality alerts. As the industry changes, your team can remain agile and adaptive, all while maintaining alert clearance rate SLAs and avoiding customer disruptions.

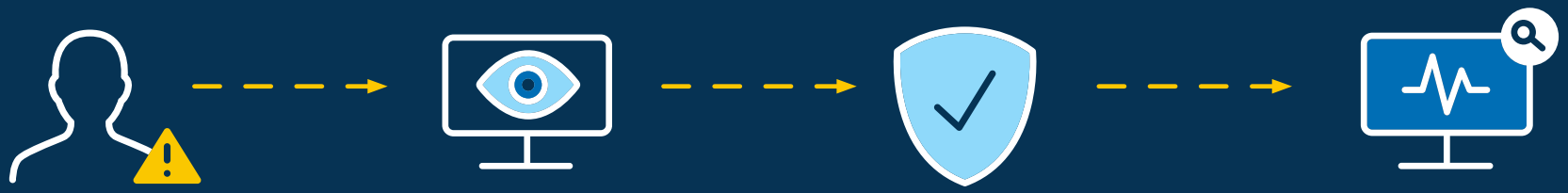
SUPPORT INVESTIGATORS

Payments Fraud Defense ingests, enriches, analyzes, and alerts on suspicious activity, finally presenting all findings to investigators within the solution's user interface.

FIGHT FRAUD

Monitor digital banking logins with DBIQ user login authentication to spot account takeover attempts. Track ACH and wire transactions to look for suspicious activity.

Payments Fraud Defense in Action: Account Takeover



A user at a global organization has their credentials stolen through an **account takeover attack.**

The bad actor is in the organization's environment, but **Payments Fraud Defense is tracking any deviation in normal behavior** — from device use, time of day, to geolocation — to flag anything suspicious.

When a suspicious transaction comes up, **Payments Fraud Defense creates an incident and blocks the transaction in real time.**

The fraudster begins making transactions while **Payments Fraud Defense monitors the amounts,** the payor and payee, and what the user session looks like.

What this means for **you**:

AS A FRAUD LEADER:
Reduce alert fatigue, improve detection rates

AS A RISK OFFICER:
Demonstrate regulatory compliance, reduce liability

AS HEAD OF OPERATIONS:
Streamline investigations, scale without additional headcount

FOR YOUR CUSTOMERS:
Faster payments, fewer false positives

The Answer isn't Working Harder, it's Seeing More

The fraud landscape has fundamentally changed. Attackers have industrialized their methods, using AI to scale their operations and target commercial customers with extraordinary sophistication. Meanwhile, banks face mounting regulatory pressure, tighter budgets, and customers who demand both seamless experiences and strong security.

The legacy approach of monitoring only the core banking system leaves you blind to the full picture. Without visibility into login patterns, user behavior, and session activity, you're making critical decisions with incomplete information — and that's exactly what fraudsters are counting on.

Fighting fraud effectively doesn't mean adding more analysts or working longer hours. It means seeing more of the attack surface before fraud happens. It means integrating detection across every layer of the user lifecycle. It means leveraging consortium intelligence, empowering your investigators with the right alerts, and stopping transactions in real time — not days later.

With **Bottomline Payments Fraud Defense**, you gain the visibility, agility, and control needed to stay ahead of evolving threats while maintaining the customer experience your commercial clients demand. The question isn't whether you can afford to upgrade your fraud prevention approach — it's whether you can afford not to.

of consumers would switch banks if their institution were linked to financial crime — and your commercial clients are likely no different.[17]

Ready to see your blind spots?

Learn more about Bottomline Payments Fraud Defense.

Learn More

Bottomline

REV US011426KV

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1 603-436-0700
Toll-free: +1 800-243-2528
info@bottomline.com