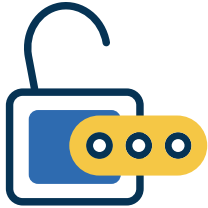




Inside the Threat You Can't Ignore

**Insider Risk Is Escalating, but
Your Bank Can Stop It**

The Data Shows a Clear and Concerning Trend



83% of organizations experiencing attacks and nearly half reporting increased frequency year-over-year¹



Credential misuse and insider-driven attacks remain one of the most expensive breach vectors, with per-incident costs approaching \$1M+ and higher for full breaches²



\$17.19M average cost when incidents take over 90 days to contain³



Banks Are Especially Vulnerable Today

Remote work, complex IT environments, and tighter regulations have expanded access while reducing visibility—while AI rapidly increases the speed, scale, and subtlety of insider activity—making threats harder to detect, contain, and control.





Today's workforce operates far beyond traditional security boundaries, expanding access while **reducing visibility** and **control**.



Remote, hybrid, and work from home models **weaken** perimeter based security



BYOD **increases risk** when personal devices lack consistent protection



Contractors and third parties function as **insiders** with privileged access



Fraud predictably **shifts** to the weakest point of protection

Modern technology environments have grown more complex, expanding attack surfaces and overwhelming traditional security controls.



Hybrid and multi-cloud IT environments create exploitable security gaps



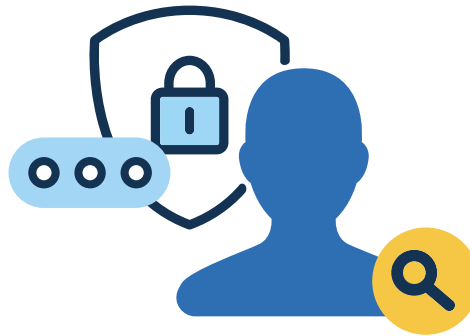
Explosive data growth makes it harder to enforce consistent access controls



Advanced tools enable stealthy, hard to detect data exfiltration



Alert overload overwhelms teams and leads to investigator fatigue



Evolving cybersecurity and privacy regulations raise the bar for insider threat programs while placing new limits on how organizations monitor and investigate users.



Cybersecurity laws mandate stronger insider threat controls and reporting



Industry regulations increase compliance complexity and oversight



Privacy laws such as GDPR restrict how monitoring data can be collected, analyzed, and retained

AI accelerates insider risk by lowering technical barriers, increasing speed and scale, and obscuring intent—making harmful activity easier to execute and harder to detect.



Generative AI enables rapid data analysis, content creation, and automation by insiders



Legitimate AI access makes malicious activity harder to distinguish from normal work



AI tools can be misused to extract, synthesize, or exfiltrate sensitive information at scale



AI driven activity increases velocity, reducing time to detect and respond

Internal fraud requires more than traditional controls, it demands continuous visibility, behavioral intelligence, and defensible investigation workflows. Expose insider fraud through continuous visibility and behavioral intelligence



Move Beyond Traditional Controls to **Expose** Insider Fraud

Internal fraud prevention demands more than traditional controls. By eliminating blind spots, banks can detect threats earlier, investigate faster, and reduce losses—**starting with these four steps.**





1. Capture the Full Picture of Insider Activity

Internal fraud often hides across systems and workflows. Banks must establish comprehensive visibility to ensure no critical signal is missed



All user activities including inquiries which typically are included in application log files



Ingest telemetry and user data from biometrics, SIEM, HR, and core banking systems



Collect activity across on premise and SaaS applications, legacy and modern



Record user events and session activity to preserve investigation context



Combine static business data with real time behavioral signals



2. Detect Risky Behavior Early

Advanced analytics identify insider fraud patterns that traditional rules and audits cannot.



Apply behavior profiling and peer group analysis to detect deviations from normal activity



Use unsupervised learning to uncover unknown or emerging fraud schemes



Leverage supervised learning and analyst feedback to reduce false positives



Prioritize threats using adaptive risk scoring and alerting

3. Investigate Quickly with Defensible Evidence

Detection alone is not enough—
banks must be able to act quickly and confidently.



- ➔ **Use visual replay** to reconstruct end to end user actions, reducing up to 90% of investigation time⁴
- ➔ **Centralize alert investigation** and case disposition workflows
- ➔ **Preserve evidence** to support internal action, audits, and regulatory scrutiny



4. Accelerate Resolution with Context and Automation

Context rich investigations reduce time to resolution and improve confidence in outcomes.

- ➔ **Deploy AI assisted agents** to generate clear, consistent investigation narratives
- ➔ **Correlate actions across systems** to establish intent and scope
- ➔ **Enable faster, more consistent decisions** across fraud, security, and compliance teams

Move beyond reactive controls.

See how Bottomline helps banks detect and stop internal fraud faster.

Request a Demo



1. IBM 2024
2. Insider Risk Statistics, 2026
3. Insider Risk Index, 2025
4. Bottomline customer portfolio data



REV US061626KV

© Copyright 2015 - 2026 Bottomline Technologies, Inc. All rights reserved.

Bottomline, Paymode, and the Bottomline logo are trademarks or registered trademarks of Bottomline Technologies, Inc. All other trademarks, brand names or logos are the property of their respective owners.

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