Bottomline

The Five Pillars of Insider Threat Prevention:

Strengthening AML & Fraud Programs from Within

Insider Threats Matter Now More Than Ever

During the past several months, multiple news stories have illustrated how insiders – whether motivated by financial gain, coercion, or negligence – can facilitate money laundering activities in ways that external criminals simply cannot.

This issue has come into sharper focus following the record $3.1 billion fine imposed on a leading U.S. bank for an AML violation - where the employee tasked with mitigating risk, exploited their position to issue dozens of debit cards linked to fraudulent accounts. These accounts were used to launder millions in narcotics proceeds through ATM withdrawals in Colombia. This demonstrates how a single rogue employee can compromise a bank's financial integrity and highlights the need for stringent internal monitoring.

Another case in the UK involved a bank manager who, along with an accomplice, opened 394 fraudulent business accounts, laundering over £7.3 million. This situation underscores the necessity for continuous risk assessment and real-time monitoring to detect anomalous employee behavior before significant losses occur.

Both these cases involved **malicious insiders,** i.e., employees or contractors who knowingly facilitate money laundering in exchange for financial gain or under duress. But money laundering can also be the result of negligent insiders or compromised insiders. **Negligent insiders** are staff members who, through poor training or lack of oversight, inadvertently enable money laundering schemes. **Compromised insiders,** on the other hand, are employees whose credentials are stolen and used by cybercriminals to conduct fraudulent activities.

Regarless of whether money laundering is the result of malicious, negligent, or compromised insiders, the implication is the same: financial institutions need to engage in proactive oversight and strategic intervention. **Following recent enforcement actions for Bank Secrecy Act violations and money laundering, the U.S. Department of Justice (DOJ) stated unequivocally to banks that:**

"...you are the first line of defense. When you criminally fail to protect your own bank from money laundering you put our financial system at risk, and we will hold you accountable."

Several key regulations emphasize the need for stronger insider threat management:

- The U.S. Bank Secrecy Act (BSA) and the AML Act of 2020 require financial institutions to implement comprehensive risk assessments, employee due diligence, and whistleblower protections.
- The European Union's 6th Anti-Money Laundering Directive (6AMLD) expands criminal liability to enablers of money laundering, including bank employees who facilitate illicit transactions.
- The Financial Action Task Force (FATF) has reinforced the importance of internal controls and enhanced employee monitoring as part of global AML compliance efforts.

Building a Robust Insider Threat Program

Establishing an internal threat program is no small task. Financial institutions must draw upon expertise from across the organization and put in place end-to-end protections. Below are five essential pillars to consider when constructing an insider threat program to combat money laundering.

1. Employ Multi-Disciplinary Expertise

One of the first hurdles in developing an insider threat program is determining who should lead the initiative. Different stakeholders within an organization – fraud teams, IT security, legal counsel, HR, and even law enforcement liaisons – bring unique perspectives to the table. Of course, each discipline leans toward its own area of expertise which can make it difficult to establish a unified approach. For instance, fraud teams focus on financial anomalies, IT security prioritizes access control, HR evaluates employee behavior, and legal ensures compliance with regulations. Without coordination, these departments may operate in silos, reducing the effectiveness of insider threat detection.

> **Insider Threat Mitigation in Action:**
>
> While collaboration is key, there must be clear leadership to drive the initiative forward. Depending on the organization's risk landscape, different teams may take the lead, but all perspectives must be represented. A well-structured insider threat program ensures that gaps in one area are balanced by expertise in another. Regular cross-departmental meetings and a centralized governance structure can help keep efforts aligned and prevent insider risks from slipping through the cracks.

2. Tailor Risk Assessments by Role and Access Level

Many organizations apply a one-size-fits-all approach to risk profiles, failing to recognize the varying levels of exposure among employees, contractors, and third-party vendors. But not all individuals within an organization pose the same level of risk. For instance, an entry-level employee with limited system access does not require the same scrutiny as a high-level executive handling sensitive financial data or an external vendor with privileged access to core systems. By failing to tailor monitoring efforts to reflect these distinctions, businesses waste valuable resources on low-risk individuals while potentially overlooking high-risk behaviors that could lead to fraud, data breaches, or compliance violations.

> **Insider Threat Mitigation in Action**
>
> A strategic approach involves implementing a segmentation model that applies different risk tolerances to different groups. Employees should be categorized based on their job function, system access level, and exposure to financial transactions. For example, an employee in accounts payable handling wire transfers should be subject to stricter monitoring than a marketing associate with no financial responsibilities. By categorizing individuals based on their roles, access levels, and interactions with sensitive data, financial institutions can prioritize their monitoring efforts and generate higher-quality alerts, reducing false positives and improving investigative efficiency.

3. Conduct Continuous Risk Assessments

Risk assessments are often conducted at set intervals – annually, semi-annually, or quarterly. However, insider threats evolve continuously, and static assessments fail to capture emerging risks in real-time. For instance, an employee's risk profile may change overnight due to financial distress, job dissatisfaction, or external coercion. If risk assessments are only performed periodically, organizations may miss critical warning signs.

> **Insider Threat Mitigation in Action**
>
> Advanced analytics and machine learning technologies should be leveraged to conduct continuous, real-time risk assessments. By integrating internal data sources – such as employee behavioral analytics, access logs, and transaction monitoring – institutions can maintain a fresh and evolving risk profile for insiders. Real-time data ingestion enables organizations to detect anomalies as they arise, rather than after damage has been done. Continuous risk assessment tools can also adapt to evolving threats, learning from past incidents to refine detection algorithms and improve accuracy over time.

4. Leverage the Power of Deterrence

While prevention is the ultimate goal, deterrence plays a crucial role in mitigating insider threats by creating an environment where employees think twice before engaging in malicious or negligent activities. When individuals are aware that their actions are being closely monitored, the risk of detection and its subsequent consequences serves as a strong disincentive.

> **Insider Threat Mitigation in Action**
>
> Business application monitoring tools that track user activity in key systems are of primary importance. This includes monitoring access to sensitive data, tracking high-risk transactions, and flagging unusual behavior patterns. Transparency is crucial: employees should be made aware that monitoring is in place, as this can serve as a powerful deterrent. By making it known that unauthorized actions will be detected, financial institutions can proactively reduce the likelihood of insider-driven money laundering.

5. Engage in Real-Time Behavioral Analysis

Traditional log-based monitoring has been the cornerstone of insider threat detection for years. While valuable, it is no longer sufficient to combat sophisticated money laundering tactics. Log-based monitoring relies on retrospective analysis, meaning that suspicious activities may only be detected long after the damage is done. This creates a reactive security posture rather than a proactive one.

> **Insider Threat Mitigation in Action**
>
> Financial institutions should adopt real-time behavioral analytics tools that provide immediate insights into user activities. These tools should be non-invasive to comply with regional privacy laws while offering advanced search capabilities across the entire employee base. Real-time behavioral monitoring enables organizations to identify unusual patterns as they emerge, allowing for immediate intervention. Machine learning-driven anomaly detection can help flag subtle deviations in employee behavior that might indicate illicit activity. Additionally, the ability to track actions across multiple systems simultaneously can reveal hidden connections and uncover complex money laundering schemes.

A holistic insider threat program:

- **Detects** suspicious behaviors in real-time
- **Prevents** illicit activities before they occur
- **Deters** potential bad actors through visible security measures
- **Ensures** regulatory compliance
- **Protects** organizational integrity

Controls should prevent and deter employees from:

- Accessing or using systems in an unauthorized or illicit manner
- Accessing or using customer accounts in an unauthorized or illicit manner
- Soliciting or receiving bribes or kickbacks, gratuities or gifts in exchange for conducting certain activities
- Conducting or processing transactions in a manner designed to circumvent compliance and reporting requirements under the BSA
- Assessing separation of duties within applications to account for job function movement or increased responsibilities for an individual or team

The Future of Insider Threat Prevention

An internal threat program to counter money laundering is never a "set it and forget it" entity – even a robust program based on the five pillars discussed above. As regulatory expectations continue to evolve, financial institutions must remain proactive in adapting their AML strategies to counter insider threats. Looking ahead, several key trends are likely to shape the future of insider threat detection:

1. **Integration of AI and Predictive Analytics:** AI will play an increasingly vital role in identifying patterns indicative of insider threats. By analyzing vast amounts of transactional and behavioral data, predictive analytics can preemptively identify potential risks before they escalate.

2. **Greater Collaboration Between Financial Institutions and Regulators:** Public-private partnerships will be critical in addressing insider threats. By sharing threat intelligence indicators and best practices, financial institutions can collectively strengthen their defenses against internal and external financial crime.

3. **Insider Threat-Focused Compliance Frameworks:** Future regulations will likely mandate that financial institutions dedicate specific resources to insider threat detection, integrating these efforts into broader AML, fraud and cybersecurity programs.

Additionally, the role of payment partners in the fight against money laundering and insider fraud cannot be minimized. Partnering with these organizations gives banks access to crucial skills, data, and detection capabilities. Incorporating this information and expertise into an internal threat program can further help prevent fraud before it happens.

An Urgent Call to Action

Insider threats are an undeniable risk in the fight against money laundering. Compliance professionals cannot afford to rely solely on external threat detection mechanisms. Instead, financial institutions must build resilient, dynamic insider threat programs that leverage technology, multi-disciplinary expertise, and proactive deterrence strategies.

The message is simple: your biggest vulnerability may already be inside the organization. The time to act is now. By implementing a robust insider threat framework, you can strengthen your defenses, enhance regulatory compliance, and safeguard the integrity of the global financial system.

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