Treliant®

From

THE PULSE

OUTLOOK 2024

Financial Crimes in 2024: Expect More Threats, Oversight, and Technology for Good and Bad

By Tyler Langenkamp, Efren Alba, Daniel Lane, and Conor Stanhope

Tyler Langenkamp
Managing Director
Treliant

Efren Alba
Engagement Director
Treliant

In today's rapidly evolving regulatory landscape, financial institutions (FI) continue to find themselves at the forefront in the fight against increasingly complex and more sophisticated financial crime. As we step into 2024, the challenges confronting FIs necessitate adoption of a proactive and adaptive approach to risk management. Financial crimes have expanded beyond traditional money laundering to include digital methods, cyber threats, and fraud. These emerging risks demand that FIs reassess and prioritize their strategies for safeguarding their operations and the integrity of the financial system.

(continued on next page)

This article delves into key financial crime priorities banks and other financial services companies should be aware of and focus on in the coming year, along with a deeper dive into four topics. As FIs brace themselves for the challenges ahead, a comprehensive understanding of the evolving threat landscape is crucial to staying ahead of the curve.

Top 10 List

1. **Beneficial Ownership**
   When discussing top-of-mind compliance priorities for 2024, most FIs will be quick to reference the implementation of the Financial Crimes Enforcement Network's (FinCEN's) beneficial ownership reporting database. The updated requirement, under the Corporate Transparency Act, will increase obligations for large and small financial institutions alike. The burden will include implementing revised customer due diligence processes and responding to increased expectations from examiners. (See section below for more details.)
2. **Banking-as-a-Service / Third-Party Risk Management**
   Banking-as-a-Service (BaaS) and other third-party relationships maintained by banks and other financial institutions have been of particular interest to regulators. The trend is likely to continue in 2024. Partnering with third parties for strategic business purposes, or to facilitate execution of certain compliance functions, can be valuable to institutions. Yet these partnerships carry unique BSA / AML and sanctions risks. (See section below for more details.)
3. **Sanctions**
   With countries increasingly using sanctions as a foreign policy tool, as well to combat money laundering and terrorist financing, many companies today are struggling to manage sanctions screening and risk. Companies need to have a game plan to keep their sanctions program current and up to date with the requirements of the Office of Foreign Assets Control (OFAC) and other anti-fraud agencies.
4. **Supervised Machine Learning Models and Transaction Monitoring**
   Regulators have continually supported, if with more than a little caution, the implementation of technologically innovative solutions for identifying financial crime typologies and mitigating risks, including supervised machine learning (ML) models in transaction monitoring (TM) systems. In 2024, FIs should consider dedicating resources to the development of more advanced capabilities in their monitoring programs, with the goal of more efficiently identifying unusual behavior and reducing false positives. (See section below for more details.)
5. **KYC / Identity Verification / Perpetual KYC**
   Financial institutions' continued emphasis on the digital consumer experience has driven a proliferation of tools for non-documentary identity verification such as "no-touch" know your customer (KYC or eKYC), real-time authentication, and

(continued on next page)

Daniel Lane
Director
Treliant

Conor Stanhope
Senior Manager
Treliant

automation of continual updates known as perpetual KYC. Regulators will likely be interested in how institutions of all kinds tune the parameters of these tools to effectively verify identities and mitigate financial crime risks without establishing an in-person relationship with the customer. Banks and other financial institutions will need to balance initiatives that improve the ease and speed of customer touchpoints with appropriate compliance controls.

The implementation of effective model risk management practices will be crucial in helping to measure the performance and effectiveness of AI / ML models.

6. **National Priorities**
   FinCEN's published national priorities provide a strategic framework that enables a more focused and effective allocation of resources, fostering a coordinated and proactive approach to mitigate emerging threats and vulnerabilities within the financial system.

7. **Risk Assessment**
   The landscape of BSA / AML and sanctions risks continues to evolve toward more complex and unique typologies. Banks and other institutions will need to take steps to consider how their risk profiles are impacted through the execution of robust BSA / AML and sanctions risk assessments (supported by tailored, quantitative methodologies). This will be particularly relevant to banks looking to expand their offerings to match the ever-growing demand for digitally enabled banking products and services.

8. **Model Risk Management in the AML Space**
   2024 promises to advance the role that artificial intelligence and machine learning (AI / ML) models play in assisting FIs in the identification and mitigation of money laundering and sanctions risks. Alongside this development, the implementation of effective model risk management practices will be crucial in helping to measure the performance and effectiveness of AI / ML models to determine whether the design concepts remain sound and achieve their stated objectives. (See section below for more details.)

9. **Enforcement Action Outlook**
   Looking to 2024, key marketplace and geopolitical developments will continue to pressure Congress and regulatory agencies to increase supervision and enforcement actions, especially surrounding lending activities, FinCEN's new beneficial ownership requirements, and ever-changing global sanction lists. In the wake of the highly public bank failures of early 2023 and during international conflicts, the need for banks to work toward remediating outstanding supervisory findings and building proper control environments will be paramount to avoid the escalation of supervisory scrutiny.

(continued on next page)

10. Internal fraud considerations

Financial institutions are increasingly exposed to different types of fraud, through ever-evolving fraud schemes and typologies. Even as the methods to combat these risks become more sophisticated, 2024 may bring a threat closer to home—internal fraud. (See section below for more details.)

Deeper Dive

Beneficial Ownership

On January 1, 2024, reporting companies in the United States will begin to fulfill the Beneficial Ownership Information (BOI) requirements of the Corporate Transparency Act. With certain exemptions, reporting companies are defined as those generally created by a filing with a secretary of state, tribal, or similar office. These include limited partnerships, limited liability partnerships, and business trusts, in addition to corporations and LLCs. Under the rule, a beneficial owner includes any individual who, directly or indirectly, either (1) exercises substantial control over a reporting company, or (2) owns or controls at least 25% of the ownership interests of a reporting company. Reporting companies created or registered before January 2024 must file their initial reports prior to January 1, 2025, with reporting companies created or registered on or after January 1, 2024, required to file their initial report within 30 days after receiving notice of their creation or registration. The reporting requirements are generally consistent with FinCEN's final rule on customer due diligence (CDD), and may not impose a substantial time burden on reporting companies. FinCEN estimates that information collection and filing time required will range from 90 minutes for simple ownership entities to 650 minutes for complex entities.

With the additional FinCEN reporting requirements, Treliant expects that implementation of BOI reporting will increase examiner expectations regarding the CDD, Enhanced Due Diligence (EDD), and suspicious activity reporting (SAR) controls of U.S. financial institutions. FIs should note certain potential downstream impacts to existing controls:

New beneficial ownership rules will increase examiner expectations regarding CDD, EDD, and SAR controls.

(continued on next page)

The OCC has specified bank partnerships with fintechs and other third parties as an area of primary examination focus.

BSA / AML Area of Interest	Potential Impact Requiring Assessment & Investigation
Risk Assessment	· An FI's risk assessment may not identify exposure to higher-risk entity type customers and counterparties and the FI's corresponding controls.
Customer Due Diligence	· As the BOI reporting final rule specifies that a reporting entity must identify one beneficial owner even if the owner's percentage ownership is less than 25%, current KYC / BOI collection, CDD data structure, and ownership percentage threshold validation rules may not allow for overrides to identify one owner nor sufficient data capture of additional owners with percentage ownership below the 25% threshold. · Monitoring OFAC sanctions, screening names of politically exposed persons (PEP), and tracking negative news watchlists may not provide comprehensive party coverage. · Written CDD and EDD procedures and policy statements may not reflect the BOI reporting requirements. · FIs may have potentially higher-risk customers that are legal entities registered in U.S. states with high corporate secrecy (e.g., Nevada, Delaware, Wyoming, South Dakota) or that are structured as special purpose vehicles (SPVs), family offices, family investment LPs, or LLCs that are not subject to EDD based on the FI's customer risk rating model and that may not comply with the BOI requirements.
Suspicious Activity Reporting	· Automated and manual transaction monitoring may not identify potentially suspicious activity involving higher-risk entity customers or counterparties. · Written investigation procedures may not reflect the BOI reporting requirements.
Training	· KYC, TM investigations, and other BSA training may not incorporate BOI requirements.

To implement the BOI implementation, FIs should visit FinCEN's Beneficial Ownership Information website and review the final rule, FAQs, and small entity compliance guide to develop an understanding of reporting requirements and potential customer impact. Based on a gap assessment, FIs should enhance existing BSA program components as necessary to align with BOI reporting requirements. As always, FIs will be expected to continue to identify and remediate CDD collected information data quality and data completeness deficiencies to ensure an effective KYC control environment.

(continued on next page)

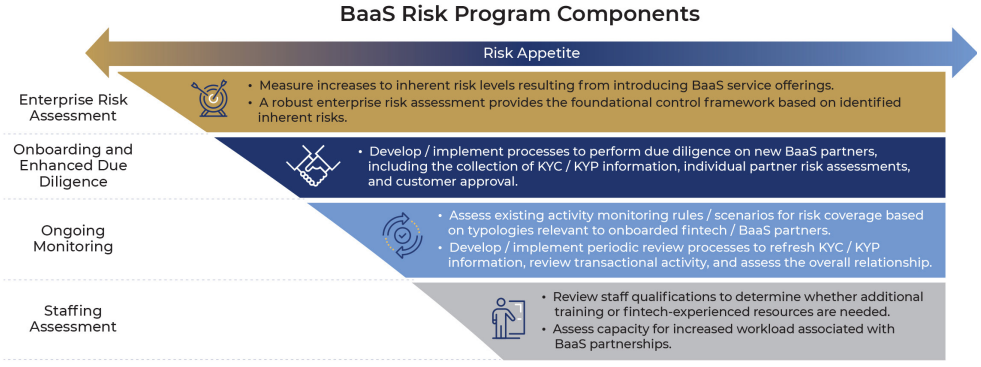
BaaS / Third-Party Risk Management

Regulators have consistently signaled an interest in financial institutions' ability to manage BSA / AML and sanctions risks arising from partnering with third parties, particularly as it relates to the creation of BaaS programs. In its 2024 Operating Plan, the Office of the Comptroller of the Currency (OCC) outlined its key operational objectives for the Committee on Banking Supervision, specifically highlighting bank partnerships with fintechs and other third parties as an area of primary examination focus.

Other regulatory bodies have also emphasized the importance of third-party / BaaS risk management, evidenced by a consent order issued jointly by the Federal Reserve and the New York Department of Financial Services (NYDFS) to Metropolitan Commercial Bank over its AML controls related to third-party programs. Several agencies also recently published interagency guidance focusing on the lifecycle of risk management for banks engaging with third parties.

From a BSA / AML and sanctions standpoint, the risks of BaaS and other third-party programs generally arise from a decreased ability for the bank to understand the nature of "end-users," i.e., the customers of the partner. Fintechs or other strategic partners are often not licensed financial institutions themselves and are not bound to the same KYC or other BSA / AML-related protocols typically imposed on traditional banks. As a result, banks looking to engage in strategic partnerships with third parties must implement a robust third-party risk management (TPRM) program that both thoroughly understands the nature of the partner's customer base and ensures the adequate execution of BSA / AML and sanctions controls performed by the partner (where applicable). The BSA / AML and sanctions components of an effective TPRM program should be governed by a defined risk appetite statement, determined by the board of directors and senior management, and accompanied by an enterprise-level BSA / AML and sanctions risk assessment that considers potential impacts on the bank's risk profile resulting from third-party offerings as follows:

BaaS Risk Program Components



Financial institutions continue to struggle to meet efficiency and effectiveness objectives with rule- and scenario-based transaction monitoring.

(continued on next page)

In addition to implementing a robust set of controls that assess, monitor, and control for potential BSA / AML or sanctions risks posed by engaging in strategic partnerships, banks should also maintain documented processes covering:

- **Limits**: For each strategic partnership, banks should establish limits and associated controls on certain customer types, transaction methods, volumes, and geographies, based on the risk posed by the partner.
- **Contract Negotiation**: Banks engaging with strategic partners should ensure careful documentation of roles and responsibilities, particularly where partners plan to execute BSA / AML or sanctions functions on behalf of the bank.
- **Termination Practices**: In the event a strategic partnership is no longer beneficial to a bank, or becomes outside of its risk appetite, the institution should maintain specific processes to wind down and ultimately terminate services offered through the partner.

Overall, any institution engaging in strategic partnerships, through BaaS or other arrangements, should consider the lifecycle of the partnership in the design of TPRM programs, from initial risk assessment to termination.

Financial institutions should continuously assess opportunities to apply ML models to drive the effectiveness and operational efficiencies of transaction monitoring.

Supervised Machine Learning Models and Transaction Monitoring

Financial institutions continue to struggle to meet efficiency and effectiveness objectives with rule- and scenario-based transaction monitoring. Both internally developed and external vendor models consistently generate high levels of false positives (FP), requiring a substantial commitment of investigative resources to review, disposition, and document unproductive alerts. FIs are required to review and process alerts in a timely manner and with sufficient rationale and documentation to support decisioning, even with FP alert rates often exceeding 90%. In an effort to reduce BSA / AML operational expenses and avoid operational backlogs, banks are increasingly outsourcing first-level alert review to third-party service providers in lower-cost near-shore and off-shore locations.

The Interagency Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing (December 3, 2018) encouraged banks to "consider, evaluate, and, where appropriate, responsibly implement innovative approaches" to meet their BSA / AML compliance obligations. As an example, the joint statement referenced the use of AI in transaction monitoring systems as an example of an innovative technology. Financial crime compliance industry approaches to TM include supervised and unsupervised ML models comprised of features such as assignment of a SAR event probability score, alert "hibernation," and network (cluster and link) analytics. Within the investigative process, natural language processing (NLP) and large language model (LLM) use cases focus on driving efficiencies in compiling and organizing required investigative information.

(continued on next page)

Data science and data analytics are critical in supporting TM ML models that require numerous enriched data attributes including channel, geography, customer, product, and external risk reference sources. To prepare for introduction of ML models and to ensure effective TM ML model deployment, banks should assess current and planned data repositories for data quality and completeness of transaction, customer, account, and reference data.

In response to the higher complexity of TM ML models, banks may be held to increased scrutiny within their model risk management environment, especially regarding TM ML model bias detection and explainability. This requires a clear set of model definitions and precise performance and monitoring requirements, including metrics and thresholds for effective TM ML model governance. Independent model validation will likely set a high bar for model documentation of the ML algorithm.

The vendor landscape has continued to expand with multiple market participants offering a wide variety of AI / ML approaches. FIs should continuously assess opportunities to apply TM ML models to drive effectiveness and operational efficiencies. Implementation of TM ML models is often associated with reductions in the number of false positive alerts requiring human intervention and prioritizing alerts by the likelihood of a SAR filing, thereby allowing FIs to adopt a more efficient risk-based approach to transaction monitoring, reducing the SAR cradle-to-grave lifecycle while enabling timelier suspicious activity reporting to regulators and law enforcement.

Internal Fraud Considerations

Financial institutions are experiencing ever-increasing rates of fraud, mainly caused by advances in technology, economic stressors, and surges in organized crime. In most cases, FIs are deploying more sophisticated techniques and controls to detect and prevent fraudulent transactions initiated by external threats. However, the greatest fraud risk that institutions face may not be organized crime syndicates, but someone who walks into a company office or branch location every morning.

The Association of Certified Fraud Examiners' (ACFE) Occupational Fraud 2022 report assessed 2,110 cases of internal fraud from 133 countries, which led to estimated losses of $3.6 billion. Banking and financial service organizations accounted for nearly 17% of examined cases, with a median financial loss of $100,000.

The ever-growing threat of internal fraud requires strong internal controls and solid strategies. Institutions of all sizes should be assessing their programs, analyzing gaps / weaknesses, developing internal controls, and updating policies and procedures. The following information outlines the key warning signs that leadership should be aware of, most common types of internal fraud, and actionable prevention strategies that institutions can employ to combat internal fraud.

The ever-growing threat of internal fraud requires strong internal controls and solid strategies.

(continued on next page)

Onboarding programs are critical and ideal opportunities to promote core values of honesty and integrity and demonstrate a zero-tolerance policy.

Warning Signs of Internal Fraud

Some of the largest and highest-profile cases of internal fraud are committed by employees that hold positions of trust and have access to sensitive information. The signs of internal fraud vary based on the type of fraud being committed but if any of the following red flags occur, it may be time to investigate:

1. Activity in dormant / elderly customer accounts
2. Increase in customer complaints
3. Unused employee vacation time
4. Employees under increased pressure
5. Circumvention of controls
6. Unjustified increases in expense activity / unusual invoice patterns

Examples of Internal Fraud

Internal fraud can occur at various stages of the customer experience and in different areas of responsibility. Some of the most prevalent types of internal fraud include the following:

1. Transaction reversal by tellers
2. Account manipulation
3. Account takeover
4. General ledger fraud
5. Loan fraud
6. Internal collusion
7. Data theft
8. Credit abuse
9. IT access control manipulation

Internal Fraud Prevention Strategies

To protect financial institutions from fraud, leadership must be vigilant in fraud detection and prevention efforts. In addition to considering external fraud threats, consideration should be given to internal threats as well.

Below are some strategies an FI can use to minimize, prevent, or control the risk of internal fraud loss events.

1. Employee Background Verifications

Verifying new employees before onboarding them can help reduce fraud risks significantly. This can be done through a host of digital pre-onboarding checks that are fast and efficient. Background checks for the banking industry cover the following aspects:

- Identity
- Address
- Education

(continued on next page)

- Past employment
- Court filings
- Criminal records

2. Employee Knowledge of FI's Culture

Onboarding programs are critical and ideal opportunities to promote core values of honesty and integrity and demonstrate a zero-tolerance policy. In addition, the reference to examples of reprimanded or fined employees who engaged in fraudulent activities and suffered the consequences for inadequate job performance, can also be a preventive control.

3. Internal Fraud Reporting Channels

Having a trustworthy source to tip you off can help management more quickly and save the damage that comes with fraud. Co-workers can often tell when someone is committing internal fraud. However, they don't necessarily want to report the information because they may be afraid of retaliation from both the perpetrator and company leadership. Consider setting up a communication channel such as a phone hotline or a website that allows people to report issues anonymously.

4. IT Security Controls

- *Mandatory System Log Out*

Employees who intend to commit fraud tend to access the system when no one is watching. The best time for this is post-working hours. It is important for employees with access to sensitive information to log out and prevent misuse of the data.

- *Password Protection Policy*

Employees could abuse their authority and access to the general ledger accounts to transfer funds from one account to another. While widely recognized as a bad policy, sharing of login credentials is very common and can be a sign of suspicious activity. One of the most devastating internal fraud schemes is one in which insiders collude with external fraudsters.

- *Require IT Administrators to Sign In*

IT administrators typically access networks using generic logins, making it impossible to track their activities. Management should mandate that these employees or contractors use their own credentials, to create an audit trail. Also, user access profiles should be checked and updated (as needed) on a regular basis. Consider conducting a search for employees with higher-level access than they should have as well as reviewing records to identify anyone who was temporarily given extended access that would allow them to commit fraud more easily.

FIs need to invest in their financial crime program, foster collaboration with regulatory bodies, and continually enhance their risk management frameworks.

(continued on next page)

5. Deploying Advanced Technology

As digitization improves the banking experience for customers, it also invites fraudsters to use technology to cheat businesses and customers in novel ways. Therefore, a proactive approach to fraud detection and prevention is imperative to ensure customers' trust, employee compliance, and overall improvement in operational efficiency. More advanced methods based on technology can help in finding and rooting out internal fraud. These include deploying AI / ML and other advanced analytical tools.

Conclusion

As 2024 unfolds, the ever-evolving landscape of financial crime necessitates a dynamic and forward-thinking response from financial institutions. In an era of technological advancements, regulatory scrutiny, and increasing interconnectedness, the need for a robust and adaptive approach to combating financial crimes has never been more critical. The priorities outlined in this article underscore the imperative for FIs to invest in their financial crime program (via technology, hiring, and program assessments), foster collaboration with regulatory bodies, and continually enhance their risk management frameworks. Doing so will reinforce the financial sector against the persistent threats of fraud, money laundering, and cybercrime. Treliant and its professionals stand ready to help our clients navigate the waters of today's financial crime and fraud environment.

Tyler Langenkamp
Tyler Langenkamp is a Managing Director at Treliant. He has over 25 years of experience advising clients across many industries on the development of major initiatives and compliance programs related to anti-money laundering (AML) and sanctions, risk management and mapping, bankruptcy and restructuring, as well as investigations and dispute resolution. **TLangenkamp@treliant.com**

Efren Alba
Efren Marquez Alba is an Engagement Director with Treliant. His financial crime experience includes Anti-Money Laundering/Counter-Terrorist Financing (AML/CFT), sanctions, anti-bribery and -corruption, and fraud. **EAlba@treliant.com**

Daniel Lane
Dan Lane, a Director with Treliant, is an accomplished professional in corporate accounting, financial auditing, forensic accounting, regulator-directed monitorship, and financial crimes compliance. He has worked with financial institutions, publicly-traded companies, and state government agencies. **DLane@treliant.com**

Conor Stanhope
Conor Stanhope is a Senior Manager in Treliant's Financial Crimes and Fraud Solutions practice. He has seven years of experience in managing financial crime risks in the financial services industry, having helped design and improve anti-money laundering (AML) programs for large and midsized banks, payment processors, cryptocurrency exchanges, and fintech companies. **CStanhope@treliant.com**

Treliant, Compliance, Risk Management, and Strategic Advisors to the Financial Services Industry, brings to you *The Pulse,* a quarterly newsletter offering insights and information regarding pertinent issues affecting the financial services industry. This article appeared in its entirety in the Outlook 2024 issue. Other articles that appeared in this issue include:

- Enterprise Risk Management: Pivotal to Surviving and Thriving in a Year of Uncertainty
- Guideposts Mark the Way to Get Ahead of This Year's Regulatory Trends
- Banking and Capital Market Regulators' 2024 Agenda: Faster Settlements, More Centralized Clearing, Bigger Buffers

To subscribe to our quarterly newsletter, *The Pulse,* visit **www.treliant.com/knowledge-center.**

Treliant®