THETARAY

5 Best Practices for Modern Financial Crime Detection

How Banks and Fintechs Are Adapting to Complex Payment Ecosystems

Introduction

Financial institutions are rethinking how financial crime detection programs operate as payment ecosystems become more complex.

Across the US, leading banks and fintechs are adopting new approaches to improve detection accuracy, reduce false positives, and give investigators better visibility into suspicious activity across transaction networks.

Below are **five best practices** organizations are implementing to strengthen financial crime detection in modern payment environments.

1 Move Beyond Static Rules

Traditional rule-based monitoring systems rely on pre-defined thresholds and known risk patterns. While still important, these approaches often generate large volumes of alerts and struggle to detect complex or emerging financial crime schemes.

Leading institutions are adopting **AI-based behaviour monitoring approaches** that analyze activity across transaction networks, helping identify suspicious patterns that would otherwise remain hidden.

What this enables:

- **Detection of complex transaction chains**
- **Identification of hidden financial crime networks**
- **More accurate monitoring across large transaction datasets**

Why it matters? ***Modern AI transaction monitoring approaches allow compliance teams to detect sophisticated financial crime earlier while reducing unnecessary alerts.***

2 Reduce False Positives to Improve Investigation Efficiency

High volumes of alerts remain one of the biggest operational challenges for compliance teams. When investigators spend the majority of their time reviewing low-risk alerts, it becomes difficult to focus on genuine financial crime risk.

Improving detection precision allows organizations to **prioritize meaningful alerts and reduce investigation workloads.**

Key benefits:

- **Reduced investigation backlogs**
- **Faster case resolution**
- **More efficient use of compliance resources**

Why it matters? ***Improving alert quality allows investigators to focus on activity that truly warrants further analysis.***

3 Prioritize Explainable AI for Transparent and Defensible Decisions

As financial institutions adopt more advanced analytics, detecting suspicious activity is no longer enough. Teams must also understand and clearly explain why an alert was generated. Black-box models, while often powerful, can produce risk scores without clear reasoning, making it difficult for investigators to interpret results or justify decisions to auditors and regulators, particularly in highly regulated markets like the US.

Explainable AI provides visibility into the drivers behind each alert. Rather than presenting a single opaque score, these models highlight the key behaviours, relationships, and transaction patterns that contributed to the risk assessment. This enables compliance teams to interpret, validate, and confidently act on risk signals, moving beyond “what was flagged” to clearly understanding “why it was flagged.”

Key benefits:

- **Clear, traceable rationale behind alerts and risk scores**
- **Greater transparency compared to black-box models**
- **Stronger investigator confidence and faster decision-making**
- **Improved auditability and alignment with regulatory expectations**

Why it matters? ***In financial crime compliance, every decision must be defensible. Explainable systems ensure institutions can not only detect risk effectively, but also justify their actions with confidence.***

4 Improve Visibility Across Transaction Networks

Financial crime rarely occurs in isolation. It typically spans complex payment ecosystems involving multiple accounts, institutions, and jurisdictions. Yet many compliance teams still rely on reviewing individual transactions or manually piecing together connections across fragmented data sources. This makes it difficult to clearly visualize relationships and transaction flows, increasing the risk of inconsistent conclusions and overlooked patterns.

Modern detection approaches enable institutions to analyze relationships across entire transaction networks, providing a more holistic view of financial activity.

This is particularly critical in environments involving:

- **Cross-border payments**
- **Correspondent banking relationships**
- **Fintech partner ecosystems**

In the US, regulatory mechanisms such as FinCEN 314(a) requests can support network analysis by helping identify connected accounts and transaction patterns, within defined regulatory constraints.

With network visualization tools, institutions can map connections, understand transaction flows, and present complex activity in a clear, visual format.

Why it matters? ***Network-level visibility enables faster, more consistent decision-making and helps uncover hidden financial crime patterns.***

5 Streamline and Automate Investigation Workflows

In many organizations, financial crime detection tools operate independently across transaction monitoring, screening, and customer risk assessment. This fragmentation forces investigators to manually gather data and piece together the context of suspicious activity. At the same time, growing transaction volumes make manual investigation processes increasingly difficult to scale. Without standardized workflows, investigations often become dependent on individual analysts, leading to inconsistent outcomes and increased QA burden.

Leading institutions are addressing these challenges by connecting detection capabilities into unified workflows and introducing automation to support investigations.

This includes:

- **Integrating transaction monitoring, screening, and customer risk data into a single view**
- **Structuring/simplifying L1/L2 investigation workflows**
- **Automatically aggregating and presenting relevant contextual data**
- **Reducing time spent gathering information across systems**

By streamlining these processes, investigators can focus on analysing suspicious activity rather than manual administrative tasks

Why it matters? ***Integrated and automated workflows improve efficiency and consistency, reducing investigation time and ensuring investigations are conducted in a standardized, auditable way.***

Learn More

If you’re exploring ways to modernize financial crime detection, discover how ThetaRay helps banks and fintechs detect hidden financial crime patterns while reducing false positives and investigation workloads.

Find out more about ThetaRay by visiting **https://thetaray.com/**

THETARAY

Empowering banks and fintechs to detect hidden financial crime with confidence.