

top features to look for in a modern fraud/BSA platform

Ensure you choose the right transaction monitoring system to protect your institution.

In today's fast-paced digital world, community banks and credit unions are often caught between the dual pressures of ever-increasing digital transaction volume and sophisticated financial criminals who are constantly evolving their tactics. Fraudsters are exploiting older, siloed systems, putting both your institution's assets and reputation at risk – especially in the era of instant payments.

For institutions with finite resources, merely trying to keep pace with these threats is no longer a sustainable strategy. To effectively protect your accountholders and communities, you need a single, unified, and intelligent defense system. Choosing the right fraud and BSA/AML transaction monitoring platform is the single most critical investment you can make.

modern fraud prevention platform must-haves

But what exactly should you be looking for? Here are the top must-have features and functionalities to prioritize when choosing a modern platform:



- **Unified Fraud and BSA/AML Monitoring (Holistic View)**

Fraud and money laundering often overlap, using the same accounts and methods. **Why it matters:** One unified platform provides a “single pane of glass” for analysts and investigators, merging all fraud-related activities (ACH, wires, faster payments, etc.) with BSA/AML monitoring. Eliminating these data silos helps ensure a comprehensive view of the accountholder’s full risk profile, which is critical for catching complex, cross-channel fraud.

- **Real-Time Capable, Cloud-Native Processing**

Instant payments like Zelle®, RTP®, and FedNow®, require instant protection. **Why it matters:** The platform should be a cloud-native solution with modern architecture that is capable of real-time processing. This is absolutely essential for stopping fraud before the funds ever leave the account, maximizing recovery potential and drastically minimizing losses.

- **Flexible Data Ingestion and Open Architecture**

Your fraud defense is only as good as the data feeding it. **Why it matters:** A modern platform should be built on open architecture and flexible APIs to easily ingest data from critical systems (core, online banking, mobile, etc.). This helps ensure a complete, accurate, and timely view of accountholder activity across various channels to reduce blind spots.

- **Behavioral Monitoring and Risk Scoring**

Fraud often involves legitimate credentials being used illegitimately. **Why it matters:** The platform should go beyond static rules by using behavioral analytics to establish baseline customer activity. It should flag deviations in habits to detect account takeover and authorized push payment fraud, which often mimics legitimate activity.

- **Explainable AI and Machine Learning**

Advanced technology should support analysts, not confuse them. **Why it matters:** A modern platform should use ML to score and predict high-risk activity. It should also include “whitebox” explainability, providing clear reasons for alerts and building investigator confidence in decision-making.



Merely **trying to keep pace** with these threats is no longer a sustainable strategy.

- **Native Integration of Fraud Typology**

Inconsistent reporting hinders the industry's ability to track and fight crime. **Why it matters:** A platform that natively incorporates industry standards, such as the Federal Reserve's FraudClassifier model, helps banks and credit unions accurately categorize "how" the fraud occurred. This standardization improves data quality, enhances internal reporting, and facilitates more effective information sharing with law enforcement.

- **Network Level Intelligence and Collective Defense**

A fraud attack on one institution is often a test run for attacks on others. **Why it matters:** Look for a platform that leverages network-level intelligence by anonymizing and analyzing data across a larger client base. This allows the system to detect emerging fraud patterns and evolving tactics faster than any single institution could, creating a powerful collective defense that benefits smaller financial institutions.

- **Adaptive Risk Scoring and Dynamic Due Diligence**

To manage risk effectively while optimizing resources, you need to ensure the level of scrutiny matches the accountholder's actual risk profile. **Why it matters:** A modern platform must provide analysts and investigators with the tools to directly influence and customize the risk scoring logic (weighing specific factors). Furthermore, the system should allow credit unions to create their own due diligence questionnaires and monitor changes in risk to determine when additional evaluation is required.

- **Direct Regulatory Reporting**

Stopping fraud means minimizing the need for regulatory reports, but when necessary, it must be easy. **Why it matters:** While focused on prevention, the platform should seamlessly support compliance by allowing users to generate, manage, and monitor Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTR). Going a step further, a modern platform should allow direct FinCEN filing of such reports, closing the loop between an effective fraud or BSA investigation and the related regulatory requirements without having to navigate multiple systems.



To effectively protect your accountholders and communities, you need a **single, unified, and intelligent defense system.**

- **Minimal IT Maintenance and Low TCO**

Focus your expert resources on fighting fraud, not managing software. **Why it matters:** Choosing a fully hosted and vendor-managed solution drastically reduces the burden on internal IT teams. The vendor handles all infrastructure maintenance, updates, and patching, ensuring your fraud team can focus 100% on protecting your institution and accountholders.

unlock the possibilities

By prioritizing these top features, your community bank or credit union can move beyond a reactive stance. You'll be able to implement a proactive, intelligent defense strategy that maximizes fraud detection/prevention, minimize losses, and ultimately protects the trust that you have built within your community! These are also among the modern capabilities you'll find in Jack Henry Financial Crimes Defender™.

If your current platform isn't providing you with everything you need from the key features above, talk to us today.



By prioritizing these top features, your community bank or credit union can **move beyond a reactive stance**.

ready to dig into more detail?

[Get in touch](#) with our experts today.

For more information about Jack Henry, visit jackhenry.com.