Quinte Financial Technologies®

Alert Management vs. Case Management Systems

Why Financial Institutions Need Both to Detect, Investigate, and Resolve Fraud Effectively

By
Mary Dishong-VanEtten
Advisor, Quinte Financial Technologies

19 Fulton Street
New York, New York 10038

(646) 813-0694
www.quinteft.com

INDEX

Introduction

Financial institutions rely on technology to identify suspicious activity and reduce fraud exposure. However, detecting potential fraud is only the beginning. Once suspicious activity is escalated, institutions must investigate the incident, document decisions, preserve evidence, track financial losses and recoveries, fulfill regulatory reporting requirements, and maintain a complete audit trail. This makes it important to distinguish between the technologies that identify suspicious activity and those that manage the case through to resolution.

Quinte Financial Technologies®

Alert Management Systems: Detecting and Assessing Risks

An alert management system continuously monitors patterns to identify indicators of potential fraud. After evaluating the customer's account history, transaction patterns, digital banking activity, deposits, ACH transactions, check activity, and device usage. When activity appears unusual or meets predefined risk criteria, the system generates an alert for further review.

Behind the scenes, alert management systems assess multiple behavioral and transactional indicators, including:

- Frequency of online banking activity
- Preferred banking channel, such as branch, ATM, or mobile deposit
- Consistency of the login device
- Alignment of the login time with historical behavior
- History of prior payments

When activity falls outside a customer's usual behavior, the system generates an alert to provide the reviewer with context on why the event was flagged. This provides a starting point to determine whether the alert should be cleared, documented, or escalated.

Executing Investigations with Case Management Systems

A case management system is designed to manage the case lifecycle after suspicious activity has been escalated. It centralizes case information such as case notes, timelines, financial impact, customer details, external parties, referrals, and other supporting documents and reporting requirements into a single, organized record. For many financial institutions, it becomes the system of record because it provides a complete view of the investigation from the initial report through case closure.

Unlike an alert management system, which focuses on identifying potential fraud, a case management system manages everything that follows. It captures case actions, records who worked on the case and when, tracks losses and recoveries as they evolve, preserves supporting evidence, and documents regulatory reporting or law enforcement referrals. By maintaining a complete record of the case, it provides the visibility, consistency, and accountability needed to support both operational decision-making and regulatory oversight.

Quinte Financial Technologies®

Key Differences

Area	Alert Management System	Case Management System
Primary Focus	Detects, prioritizes, and triages suspicious activity	Manages cases from initiation through resolution
Operational Scope	Supports alert review and risk assessment	Coordinates investigative activities, documentation, decision-making, and oversight
Information Context	Provides the data required to evaluate an alert	Consolidates all information required to manage a case in one place
Case Ownership	Primarily supports fraud analysts during alert review	Supports reviewers, supervisors, compliance teams, and other stakeholders throughout the process
Business Outcome	Reduces false positives and improves fraud detection efficiency	Delivers consistent case management and improved operational visibility

The Operational Boundaries of Alert Management

Quinte Financial Technologies®

Most of the alert management systems include basic case management capabilities. While these features help reviewers document alert disposition, maintain an audit trail, and generate operational reports, they are designed to support the alert review process rather than the full investigation lifecycle. As a result, they often lack the capabilities needed to manage fraud investigations from escalation through resolution.

The limitations become more apparent as investigations progress. Financial institutions must continuously update losses and recoveries, document external parties, coordinate investigative tasks, support law enforcement referrals, prepare Suspicious Activity Reports (SARs), and generate meaningful operational and regulatory reporting.

The need for accurate financial tracking becomes even more critical as cases evolve. In the previous years, FinCEN identified more than $688 million in actual and attempted fraud across 15,417 BSA reports over a six-month period, highlighting the importance of distinguishing between attempted losses, actual losses, recoveries, and outstanding exposure throughout the investigation.

When this information is managed across multiple systems or spreadsheets, it becomes significantly more difficult to maintain accurate, up-to-date records, increasing the risk of inconsistent reporting and reduced operational visibility.

Addressing these challenges requires more than extending the capabilities of an alert management system. It requires a purpose-built platform that enables investigators to manage cases efficiently while maintaining consistency, visibility, and regulatory compliance.

Core Capabilities for a Case Management System

A dedicated case management system supports the entire investigation lifecycle through capabilities that help investigators manage information, conduct investigations consistently, and identify relationships across cases through:

- **Centralized Investigation Records**

A case management system gives investigators a centralized view of every investigation. It combines customer and account information from core systems with information gathered throughout the investigation. This includes non-customer suspects, external accounts, attempted transactions that were stopped before processing, supporting evidence, and information required for law enforcement referrals or SAR reporting.

- **Configurable Case Classification**

Configurable case classifications enable institutions to manage investigations according to their operational and reporting requirements. Cases may be categorized by payment rail, payment type, fraud or scam types, or any other institution-defined classifications. Additionally, the system also records the source of each investigation, including alerts, customer notifications, branch referrals, employee reports, and law enforcement contacts.

- **Managing and tracking investigative work**

Configurable task lists guide investigators through required investigative procedures and document completed activities. This promotes consistency across investigations, simplifies examiner reviews, strengthens quality control, and supports staff training.

The system also links related cases through common actors, incidents, crime groups, external accounts, or fraud trends. Connecting related investigations helps identify broader fraud patterns that may not be apparent when cases are reviewed individually.

Reporting and Operational Value

A fraud case management system transforms investigation data into meaningful management and operational reports. These reports support risk committee reporting, loss analysis, staffing decisions, policy reviews, charge-off reporting, and fraud trend analysis. Reporting can be tailored by branch, region, fraud type, or other institution-defined categories, providing leadership with the visibility needed to monitor both operational performance as well as emerging risks.

A case management system also streamlines operational activities by generating standardized forms and documentation, including customer affidavits, claims documents, hold harmless requests, customer correspondence, bank-to-bank communications, law enforcement referral packages, and SARs.

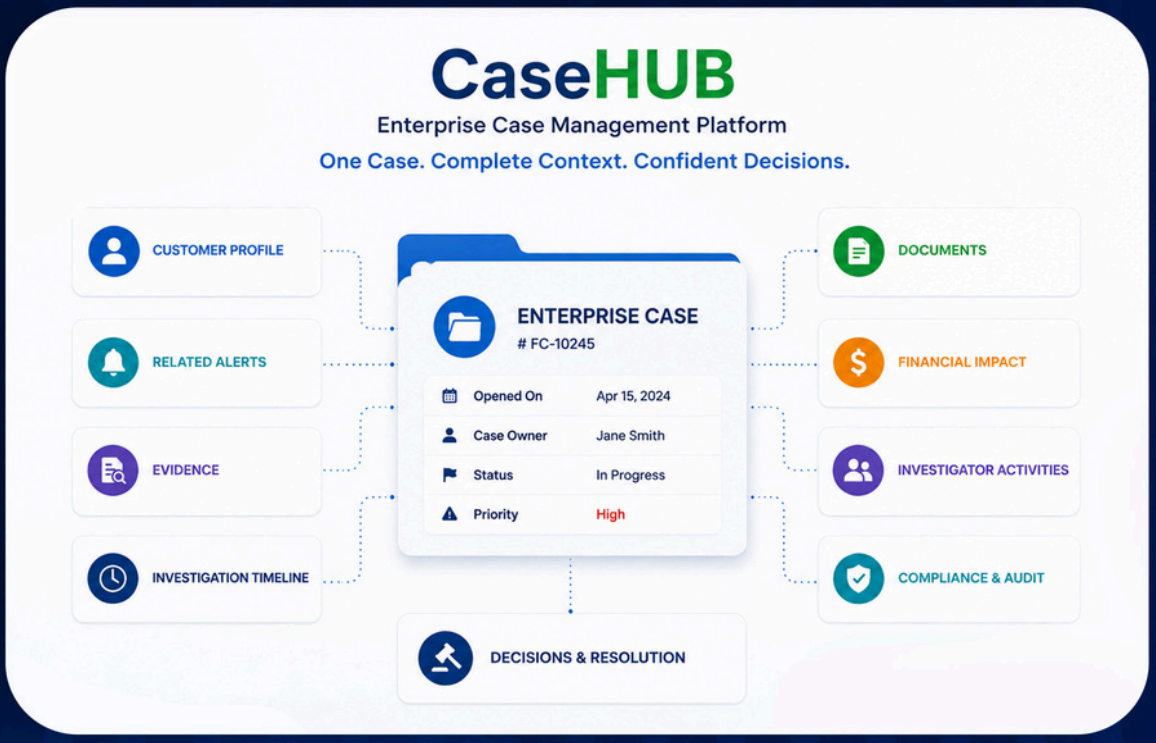
Standardized documentation improves the quality and completeness of investigative records while simplifying regulatory reporting and information sharing. With more than 87% of IRS Criminal Investigation cases recommended for prosecution supported by a BSA filing, this strongly underscores the importance of maintaining complete, accurate, and well-documented case records.

Quinte Financial Technologies®

How CaseHUB Manages Modern Fraud Operations

CaseHUB is an enterprise case management platform that enables financial institutions to manage investigations within a unified framework, connecting investigative activities, supporting evidence, regulatory requirements, and oversight throughout the case lifecycle.

It embeds automation, auditability, and governance into every stage of case execution, enabling institutions to establish consistent investigative practices, strengthen regulatory compliance, and improve visibility across fraud operations as case volumes continue to grow.



Conclusion

While both alert management systems and case management systems are important, they are also designed to address different stages of the fraud investigation process. Financial institutions should not view the choice as one versus the other. When these systems are properly integrated and configured, institutions can move from initial report or alert generation to complete resolution in a streamlined and well-documented manner.

Sources :
1. www.fincen.gov
2. https://www.fincen.gov/system/files/shared/FinCEN-Infographic-Public-2025-508.pdf