PEGA

Holistic fraud and financial crimes management: Now is the time

Improve the accuracy and efficiency of your operations

Introduction

The frequency and complexity of financial crimes is increasing

In recent decades, the evolution of fraud and financial crime detection systems was spurred by new risk trends and technology advancements. While fraud detection traditionally used artificial intelligence (AI) and machine learning techniques, financial crimes utilized complex rules engines to detect cases. Over the last several years, financial services firms have extended the capabilities of AI and machine learning to financial crimes alert management with significant results, such as reductions in false positives, improved risk detection, and increased automation at scale.

However, though fraud and financial crimes functions use similar monitoring techniques, they still largely operate independently within most financial firms. This model may have been appropriate years ago when fraud and financial crime schemes were dissimilar and managed accordingly, but current factors like channels, payment rails, and decentralization are blurring the line between fraud and financial crimes.

The Financial Crimes Enforcement Network advisory FIN-2016-A005 requires financial institutions to have line of sight into cyber events and crime – making the harmonization of fraud and financial crimes not only an opportunity for operational efficiency but also a regulatory requirement.

While blending operational practices across fraud and financial crimes has been positive to the industry, it has also led to some challenges. Financial institutions must consider:

- **How can newer fintech and legacy detection investments operate simultaneously?**
- **What does operationalizing detection and identification across fraud and financial crime teams look like?**
- **How can a reduction in manual activities be achieved with systems that have different levels of automation?**

To answer these questions, financial institutions need to evaluate the current and future challenges inherent in their existing systems.

Top 3 challenges to harmonizing fraud and financial crimes practices

1. Point solutions can't fully address institutional needs

The maturation of the fraud and financial crime landscape is far less straightforward than it was years ago. Previously disparate fraud detection and case management systems were aligned by channel, but otherwise disconnected.

Financial services firms now know that the staffing levels required to triage and service up to a 95% false positive rate of detection were unsustainable. This presented a significant opportunity for AI and machine learning. While a popular method of identification in the fraud space, only recently have AI and machine learning been deployed within banks for financial crime detection.

The market is now flooded with fintech vendors specializing in detection systems or reduction in false positives, but with one notable caveat – they are not the end-all and be-all. While those capabilities are a start, banks looking to supplement their financial crime detection and transaction monitoring systems with point solutions find that these solutions only partly address their full-scale fraud and financial crimes needs.

2. Increased costs and poor customer experience from disparate, duplicated processes and activities

Many of the detection systems in place at financial institutions are purpose-built for anti-money laundering and financial crimes. As schemes become more sophisticated and new digital channels and rails emerge, financial institutions are struggling to aggregate these risks at enterprise-scale.

Although financial crimes and fraud teams are separate at many firms, they usually serve as a centralized group function for the bank. And while they function as separate teams, most of the tasks carried out by these investigative resources are very similar. By not maximizing the overlapping nature of the tasks carried out by financial crimes and fraud teams, banks risk slower time-to-resolution, inconsistency in outcomes and decisions, and ultimately, inaccuracy.

3. Partially automated processes hinder enterprise-scale improvements

Even as detection systems improve and produce fewer false positives, part of the investigation process is still largely manual. In many financial institutions, data – whether internal or third-party – is still scattered across multiple siloed systems and requires manual intervention. This leads to inconsistencies, errors, and missed steps.

The struggle for effectiveness and efficiency increases even more if you consider the effects of disparate detection systems with differing levels of automation within their case management workflows. This does not provide a harmonized user experience for bank employees responsible for these outcomes.

The cost of duplication of work, rework, and human error should not outweigh investment in **a proper case management system to manage each step of the process.**

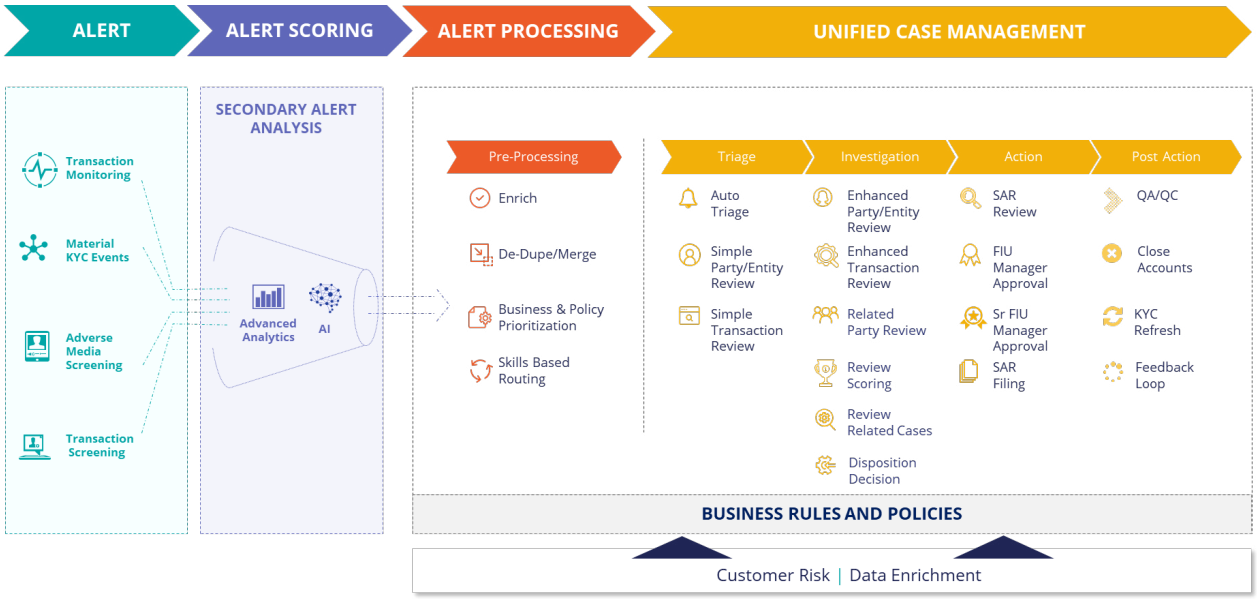
There's a better way to manage fraud and financial crimes

An enterprise framework for alerts management

In the last five to seven years, financial institutions have invested heavily in enhanced detection monitoring systems, taking advantage of capabilities from fintechs that specialize in AI and machine learning. This trend is a prime example of financial institutions using a best-of-breed approach that marries investments in legacy systems with newer, AI-based technologies.

But banks can go further to improve accuracy and cost-efficiency.

The next step is utilizing the detection output from these systems with a unified workflow and case management system.



Example of alerts and investigation management within a unified case management system

A unified approach has several advantages:

- **Consolidation of output** across multiple detection systems and improved visibility into overall risk
- **Intelligent routing** to reduce cost and touchpoints
- **Automated manual processes** so users can focus on investigative outcomes
- **Ease of integrating** new detection methods into existing processes

Advantages of a unified approach

Holistic risk oversight with aggregation and scoring of alerts from multiple detection systems

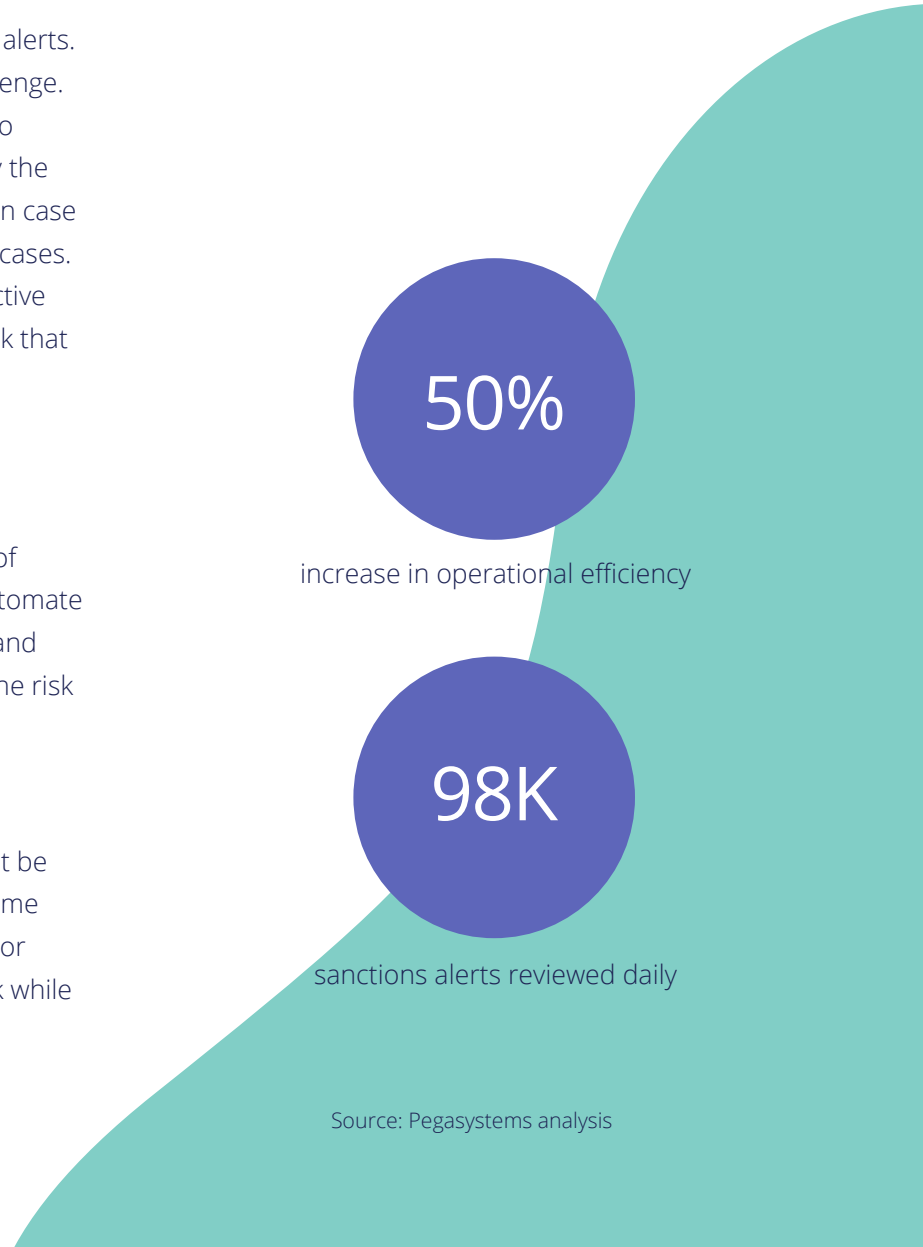
Detection systems have various scoring methods to predict the potential risk and priority of alerts. This is very useful, however, multiple scores from multiple detection systems present a challenge. A unified workflow and case management system supports industry best practice, which is to aggregate scores from various detection systems then rescore to factor in risks identified by the multiple systems. Additionally, leading financial institutions are starting to move to a common case management system for fraud and anti-money laundering (AML)/financial crimes alerts and cases. Although these alerts and case types are commonly worked on independently by the respective fraud and AML/financial crimes units, a unified system give banks visibility into the overall risk that an entity presents.

Reduced manual activities through connected data and processes

As detection systems incorporate more AI and machine learning analysis into their output, the number of false positives will decrease. Theoretically then, the number of cases worthy of investigation will increase. A unified workflow and case management system helps banks automate and streamline investigative tasks and processes, such as quickly analyzing related internal and third-party data. This allows investigators to spend their time investigating and decisioning the risk rather than gathering information to aid their investigations.

Increased productivity and accuracy with skills-based routing

As financial institutions continue to look to reduce operational costs, exposure to risk cannot be sacrificed. Whether investigative units are operating on an onshore, onshore/offshore, or some other hybrid model, the goal is to direct an alert and/or case to the analyst and/or investigator best suited for its complexity, risk, or other factors. This allows firms to properly manage risk while controlling operating costs.



Source: Pegasystems analysis

Learn how intelligent workflows are helping banks improve operations and fulfill regulatory requirements

Leading banks are now realizing that a unified approach to workflow and case management allows them to streamline back-end systems to achieve operational efficiency and fulfill regulatory requirements.

Take the next steps to learn how. Visit pega.com/industries/financial-services/financial-crimes to see how a holistic view of customer risk can help you streamline research, improve decisioning outcomes, and provide better client-centric services.

About Pegasystems

Pega delivers innovative software that crushes business complexity. From maximizing customer lifetime value to streamlining service to boosting efficiency, we help the world's leading brands solve problems fast and transform for tomorrow. Pega clients make better decisions and get work done with real-time AI and intelligent automation. And, since 1983, we've built our scalable architecture and low-code platform to stay ahead of rapid change. Our solutions save people time, so our clients' employees and customers can get back to what matters most.

For more information, please visit us at **pega.com**