

Gain a Strategic Advantage in the Fight Against Financial Crime

Enhanced analytics techniques can help financial institutions manage risk more effectively by prioritizing alerts

Financial criminals have gained sophisticated technology weapons, forcing financial institutions to strengthen their defenses and reevaluate their current technology. Fortunately, there are advanced solutions to combat the increased risk.

Financial institutions can employ enhanced analytics, machine learning and data science to protect their institutions and optimize their analysts' time. Advanced detection and alert tools enable compliance staff to focus on the highest-risk alerts so they can track and thwart money laundering and fraud.



The United Nations Office on Drugs and Crimes estimates money laundering activities equal 2 to 5 percent of global GDP or \$800 billion to \$2 trillion USD. Despite the best efforts of financial analysts, less than 0.2 percent of laundered money is detected.











In 2020, the FTC received more than 2.2 million reports of fraud, with losses totaling more than \$3.3 billion. And the problem isn't likely to recede. The COVID-19 pandemic accelerated consumers' reliance on digital services worldwide, creating more data and users for the financial sector to analyze. Criminals can exploit that increased volume to hide fraud and money laundering crimes in the boom of digital transactions.

To combat financial crime in this environment, financial institutions need to replace time-consuming, manual processes with more advanced techniques. New technologies can improve the speed, quality and efficiency of detection and help financial institutions manage crime risk at an improved rate, according to the Financial Action Task Force (FATF). In January 2021, FATF Executive Secretary David Lewis spoke about the importance of using technology to weed out criminal activity more efficiently and effectively. Big data analytics and machine learning, he said, will enhance productivity and standardize key compliance efforts.

Enhanced analytics can deliver those productivity gains and give financial institutions the boost they need to keep pace with criminals. As the financial industry plans for the future – one in which alerts and volume may outpace resources – advanced technology will be necessary. To fight financial crime, financial institutions will need to combine data science and machine learning technology to enhance detection.

Automation Opportunities

Automation can be applied to key functions throughout the financial crime risk management life cycle, which encompasses detection, remediation and reporting.

-  Alert/Case Notes
-  Alert Management
-  Data Management
-  Data Verification
-  KYC Operations
-  Managerial Reporting
-  Regulatory Reporting
-  Risk Management
-  SAR Narrative
-  Watch List Filtering

Adding the Power of Machine Learning to Human Experience

Even successful review processes can be enhanced by machine learning. Automatic alert generation can be combined with information from analysts' investigations of previous alerts and cases. This creates a symbiosis of human expertise with the technology of a machine learning model.

Automatic alerts inform the data with intelligence gathered from previous investigations. As suspicious activity is detected, data is funneled or filtered, resulting in behavioral profiles. Those profiles are studied and behavioral analytics can be performed on the data.

As data becomes more comprehensive, it begins to tell a story and build a scenario. Learned patterns of behavior can point to warning signs of financial crime. For example, there may be indications of **layering** or activities designed to create confusion. A company might suddenly change spending habits, move large amounts of money, change locations, buy new properties or undertake an expansion. Unusual activity is not necessarily an indicator of criminal activity. But with machine learning, financial institutions gain an extra filter that helps them recognize suspicious changes and interpret whether conduct is criminal.

Machine learning also assigns scores to alerts, so the most urgent cases are moved to the top of analysts' lists. This helps analysts manage their time and prioritize cases.



Applying Data Science

Financial institutions receive data from numerous sources and all of it must be ready to review and risk score. Accurate data is key to informing machine learning and to ensure the best outcomes of enhanced analytics.

It's important to use the newest data possible and to conduct a thorough cleanup before it's applied. Then, identify predictive features and information combinations to categorize alerts as productive or unproductive.

During the model-tuning and model-building stages, financial institutions can incorporate their tolerance for risk. Personalized risk levels can be built into the risk model and the application itself.

Once an informed model is created, the process can flow automatically. Data is ingested and cleansed, then given a risk score. Based on an institution's risk threshold, scores can be ranked and prioritized accordingly. The most urgent alerts are automatically sent to analysts for immediate review.



Benefits

Advanced tools provide an effective way to combat money laundering. Machine learning, data science and enhanced analytics can:

- Enable analysts to focus on high-risk alerts
- Reduce the number of false-positive alerts
- Reduce operational costs by simplifying the alert process
- Improve risk management and support risk governance requirements

Empowering Analysts With Enhanced Analytics

With enhanced analytics, financial institutions combine behavioral analytics with rules-based alerts. Then, supervised machine learning oversees data to help ensure the best possible outcomes based on previous alerts.

Enhanced analytics help analysts prioritize the most critical alerts, especially as transactions become faster and more frequent. Since automated systems filter out false-positive alerts, analysts can investigate more intelligently, too. Analysts can easily see critical information they need to perform a holistic analysis and make quick, accurate decisions.

Advanced analytics can be used to help analysts work more effectively by:


- Assigning alert scores based on previous outcomes; alerts generated from existing scenarios are automatically prioritized
- Detecting money laundering and fraud earlier, at the transaction monitoring stage; an alert is generated as soon as suspicious activity is suspected
- Uncovering behavioral trends among customers and monitored parties


Using the Data to Drive Results

In the battle against financial crime, detection must adapt with evolving risks. As transactions and data move around the world faster than ever, financial institutions are challenged to monitor for crime in real-time. By employing the latest automated innovations in risk management, financial institutions can retire outdated manual systems and processes and gain the speed and agility they need. Enhanced detection techniques provide powerful new ways to protect our institutions and the populations who need their help the most.

Connect With Us

For more information about financial crime technologies:

 800-872-7882

 getsolutions@fiserv.com

 [fiserv.com](https://www.fiserv.com)

Fiserv is driving innovation in Payments, Processing Services, Risk & Compliance, Customer & Channel Management and Insights & Optimization. Our solutions help clients deliver financial services at the speed of life to enhance the way people live and work today.

Visit [fiserv.com](https://www.fiserv.com) to learn more.