fiserv.

White Paper

A Smarter Approach to Anti-Money Laundering

Stop the Money Laundering Cycle by Using Machine Learning to Turn Data Into Insight

the speed of life®

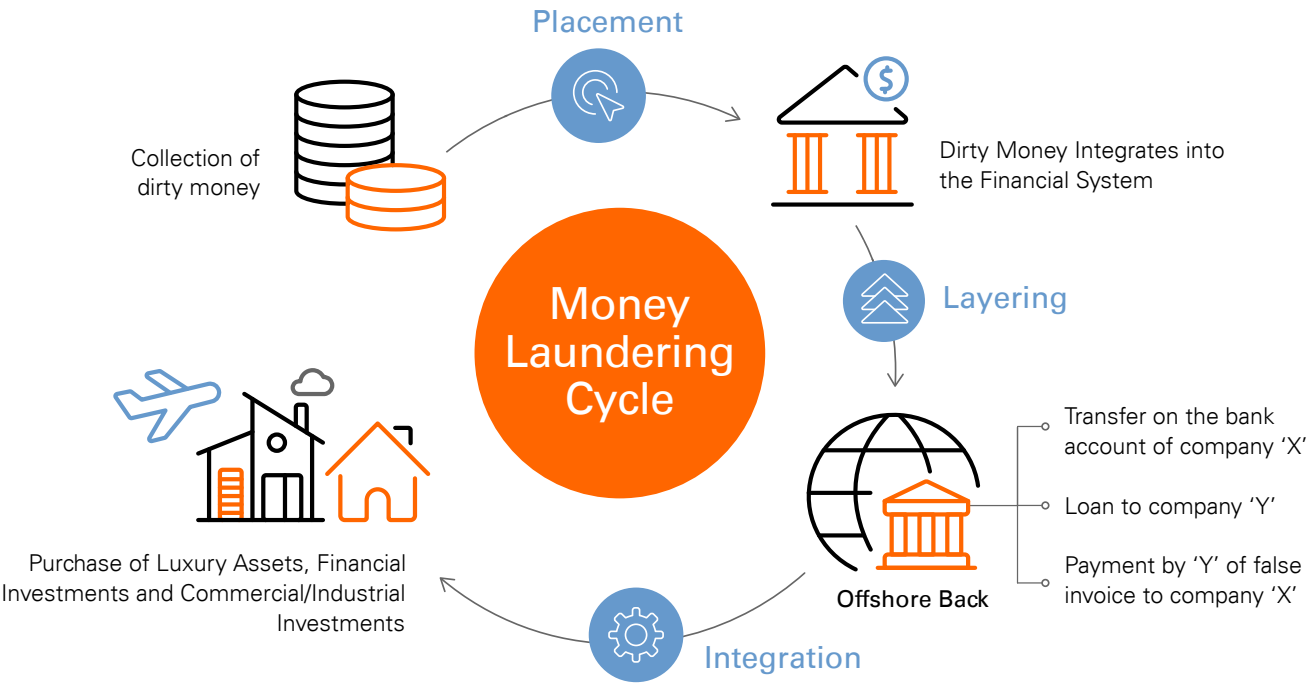
Criminals need the ability to use their illegally garnered profits without getting caught, and that's why they turn to money laundering. The scale of this problem and the rapid pace of its evolution means financial institutions must be smarter and more diligent in their anti-money laundering (AML) efforts. As the financial industry responds to new demands and prepares for the future – one in which alerts and their volumes outpace the ability of financial analysts to review them – advanced technology will play an essential role.

Although money laundering is a complex process, it generally involves three stages:

- Placement – moving the funds from direct association with the crime
- Layering – disguising the trail to foil pursuit
- Integration – making the money available to the criminal from what seem to be legitimate sources

Once criminal funds have entered the financial system, the layering and integration phases make it difficult to track and trace the money, so usually it is during the placement stage that money launderers are most vulnerable to getting caught. That's where financial analysts spend their time looking for suspicious activity – but it's not always working.

By some estimates, less than 0.2% of laundered money is detected out of activity estimated to be equal to 2% to 5% of global GDP, or $800 billion to $2 trillion USD, according to the United Nations Office on Drugs and Crimes.



Source: "Money Laundering," United Nations Office on Drugs and Crime

Financial institutions can combine the strengths of machine learning with data science techniques to create a sustainable model that better detects money laundering and reduces associated criminal activity.

Using Machine Learning to Move From Data to Insight

Even successful AML review processes can be enhanced by machine learning. Automatic suspicious activity detection leading to alert generation can be combined with information from analysts' previous investigations of alerts and cases. This creates an overlay of human expertise onto the technology within a machine-learning model.

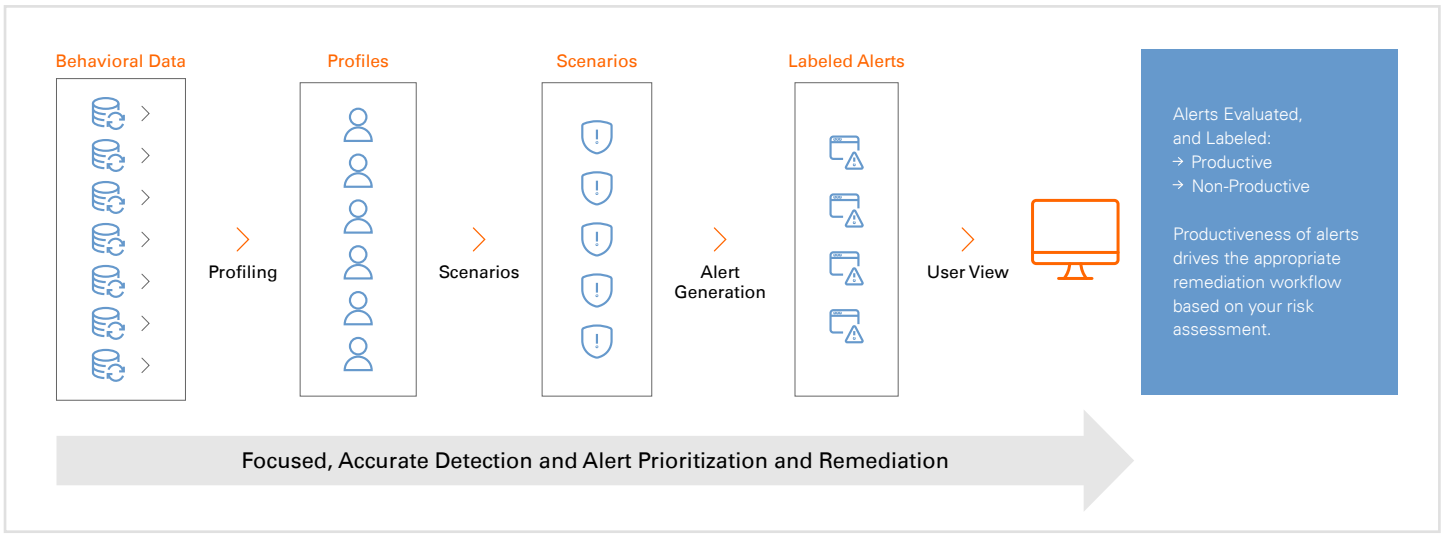
As suspicious activity is detected, data is funneled or filtered, resulting in behavioral profiles. These profiles are studied, and behavioral analytics can be performed on the data.

As data becomes more comprehensive over time, it begins to tell a story – and build a scenario. Learned patterns of behavior can point to warning signs of money laundering and predicate crimes, such as fraud.

For example, there may be indications of the layering of 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 alone 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.

Operationalizing the Approach

The data that financial institutions receive comes from numerous sources, and all of it must be ready for a machine to accept and read properly. Accurate data is key to informing machine learning and to ensuring the best outcomes of enhanced analytics. Furthermore, accurate data leads to accurate investigations that can identify the proceeds of crime. Stopping the flow of illicit funds through financial systems – and stemming the ability of criminals to turn criminal proceeds into legitimate assets – ultimately lead to a reduction in the predicate crimes for money laundering. Those crimes include nefarious activities such as human trafficking, drug trafficking and arms trading.



To intelligently apply data, it's important to use the most current data and make sure it is cleansed before it's applied. As soon as the data is in a usable form, data science techniques can be employed to identify predictive features and information combinations to categorize alerts as productive or unproductive.

Once an informed model is created, the process flows automatically – data is ingested and cleansed, then given a risk score. Based on an institution's risk threshold, suspicious activity alerts can be ranked and prioritized based on the scoring model. The most urgent alerts are automatically sent to analysts for immediate review.

With this approach to applying enhanced analytics to financial crime, financial institutions can pair behavioral analytics with rules-based thresholds and alerts.

Subsequently supervised machine learning oversees the thresholds and alerts to help ensure the best possible outcomes and achieve the goal of reducing criminal activity in the financial system.

New Tools for a New World

Financial crime detection must adapt to meet the evolving risks of the world we live in today – a world of rapid transformation in financial services, of the instant movement of money and the proliferation of digital transactions. By deploying the latest automated innovations in risk management, financial institutions can let go of outdated manual systems and processes and gain the speed and agility they need to keep up.

Connect With Us

For more information about financial crime risk management solutions from Fiserv:

800-872-7882

getsolutions@fiserv.com

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** to learn more.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045
fiserv.com

fiserv.