Emerging tech's encouraging promise: fight financial crime in real time

Financial institutions that update their digital arsenal today will stay a step ahead of crooks—and competitors.

BY ANDREW DAVIES

The quick clip of financial services innovation has gifted consumers with powerful new digital options, including faster access to their money. Yet such advances—in particular the technology underlying the services and products—can cut two ways.

On one hand, financial institutions strive more than ever to stay atop consumer innovations, both to serve customers and outflank competitors. On the other, those same innovations (such as real-time payments) can expose the financial institution and its customers to crime schemes such as fraud and money laundering.

If you think money laundering is an old-school type of crime, it may surprise you to learn that the money laundered through the global financial system has risen to between $1.6 and $3.6 trillion annually. And fines or settlements for a non-compliant U.S. financial institution can exceed $2 billion.

WHAT CAN BE DONE?

Financial crime schemes that wield the latest technologies can be fought by employing emerging technologies. Regulatory agencies—such as the Financial Conduct Authority (FCA), Financial Industry Regulatory Authority (FINRA) and Financial Action Task Force on Money Laundering (FATF)—have recently begun to promote the harnessing of innovative technologies to confront money laundering.

WHY NOW?

Global trends, new competitors and market demand push financial institutions toward an environment where they must identify money laundering and prevent fraud in real time. In addition, compliance costs and requirements continue to climb, making it even more important to rely on efficiencies gained from technology. The recently implemented regulations around beneficial ownership (where specific property rights belong to a person even though the title belongs to someone else) and verifying a client's identity through know your customer (KYC) are good examples.

Financial institutions face these hazards when they rely on older AML technology:

- *Reliance on rules-based scenarios and arbitrary threshold reporting*
- *Risk-scoring protocols based on generic attributes, which overlook unique factors surrounding a specific customer's profile*
- *Dependence on broad manual investigation by human analysts due to false alerts, rather than a focus narrowed to suspicious threats*
- *Slow technological response to added regulatory requirements opposed to a flexible, nimble approach.*

To propel financial institutions into the future, a more sophisticated approach (or combination of approaches) is necessary.

WHERE TO LOOK NEXT?

Five emerging technologies will play a bigger role in AML initiatives over the next few years:

1. Onboarding and customer due diligence biometrics and digital identification.

Years ago, customers in a physical branch could be validated through traditional means such as a driver's license. But with the advent of online onboarding, the same validation methods won't work. At the same time, customers want a streamlined, convenient onboarding process. That's where the science of biometrics comes in.

Using unique biological characteristics, biometrics identifies customers through retina scans, facial recognition, fingerprints and other attributes. Digital identity confirms through trusted sources that customers are who they say they are.

Examples include KYC identification verification using facial recognition or KYC client onboarding using biometrics and dynamic questionnaires.

2. Robotic Process Automation (RPA)

Once you've captured the customer's information, what do you do with it? RPA is an emerging form of business process automation technology equivalent to software robots or artificial intelligence (AI) workers. It increases productivity and reduces errors on highly repetitive, rote tasks, by automating:

- *Data collection for alert and case remediation and investigation*
- *Workflow for data entry and document routing*
- *Steps or deposition based on previous investigations and outcomes*
- *Regulatory reporting such as cash threshold.*

3. Natural Language Processing

Natural language processing deals with how computers process and analyze human or natural language data. Let's say a large block of text (a form, for example) needs data extracted (such as beneficiaries of payments) to drive a better understanding of anti-money laundering (AML) risk. Natural language processing can extract that data. Other examples on ideal uses include:

- *Analysis and processing of unstructured data to uncover red flag indicators in reports*
- *Understanding contextual information such as roles and relationships*
- *Collecting data points across multiple disparate sources*
- *Generating Suspicious Activity Reports (SAR) and Suspicious Transaction Reporting (STR) narratives.*

4. Machine Learning

With machine learning, systems employ models and inference when exposed to new data—getting better at the assigned task with each pass. Examples include situations in which previous history, activity and outcomes can be analyzed to predict behavior. Through machine learning, systems can:

- *Fine-tune detection based on previous alert outcomes*
- *Analyze previous alerts, thresholds and settings*
- *Improve predictive models over time*
- *Leverage the value of data, and*
- *Automate steps in the investigation process based on previous dispositions.*

5. Artificial Intelligence and Big Data

Artificial intelligence (AI) occurs when computer systems use multiple technologies to perform tasks with some of the cognitive and decision-making faculties of humans. AI can rapidly filter through large quantities of data to find risks and pinpoint when real suspicion of a money laundering threat triggers an alert. AI ranks as the go-to technology to ramp up the efficiency and effectiveness of any AML program.

HOW DO YOU START WITH NEW TECHNOLOGIES?

Ask yourself these eight key questions about your AML program; if you find it lacking, consider one or more of the technologies mentioned in this article.

- *How flexible and responsive is your system?*
- *What were the issues you experienced in previous regulatory-driven AML projects?*
- *Can your system handle the highest global AML standards while meeting today's customer standards for speed, ease and convenience?*
- *How accurate and well-maintained is your data?*
- *Are customer experience, security and compliance costs still in balance?*
- *How old are your systems?*
- *How effective is your system in facilitating and managing multiple typologies o financial crime?*
- *Is your system ready for cybersecurity incident reporting?*

Taking advantage of emerging technologies can help you overcome the limitations of aging AML technology as well as meet the challenges of a real-time environment. Weighing the benefits, your tech arsenal will experience a different brand of AML: that is, A Major Leap.

Andrew Davies is vice president, Financial Crime and Risk Management, Fiserv