Profitable defense against financial crime

BY CHERYL CHIODI

Using a holistic approach featuring automation and analytics can mitigate risk, deliver a better CX and generate revenue.

The experiences of COVID-19 in 2020 taught financial institutions that they must reimagine the way they assess and manage risk. Fraud volume keeps growing, so frontline risk teams must be empowered with the technology necessary for powerful analytics, more-robust alert management and improved accuracy.

There is no shortage of data in financial services—structured, unstructured, transactional, account-level and even behavioral—that when combined can drive insights to deliver new, customer-centric offerings. While the use of consumer data is the subject of increasing regulation, there remains tremendous potential to innovate to bring benefit to both financial institutions and their customers. However, the technological advancements that make it possible to deliver innovative products and services to banking clients can, when in the hands of nefarious actors, also make fraud more pervasive.

As financial institutions look to reset, reinvest and reimagine their business in 2021, there must be an urgent focus on effectively combating fraud through predictive analytics, robotic process automation (RPA) and natural language processing (NLP). This requires shifting the mindset from a narrow focus on false positives and loss prevention to a broader emphasis on gaining actionable insights that tangibly enhance business value.

THE BENEFITS OF BREAKING DOWN SILOS

According to the LexisNexis 2020 True Cost of Fraud™ Study, every dollar's worth of fraud costs financial services firms $3.25, up 11 percent from the previous year. Financial crime not only puts financial institutions at risk for monetary loss, but reputational damage as well.

In the financial services industry, healthy client relationships, built on a reputation of trust, translate into customer satisfaction, improved customer value and customer loyalty. Since client acquisition costs are so high—one recent study found that the average total cost for a financial advisor to acquire a new client is more than $3,000—financial crime prevention and reputational protection have a significant impact on a financial institution's bottom line. By converging fraud, anti-money laundering (AML) and cybersecurity, financial institutions can consolidate data across historically isolated functions for a more holistic view of risk.

With significant similarities in the data collected across AML, fraud and cyber teams, breaking down these silos can provide a more transparent view of the threat landscape, better detect suspicious transactions and streamline investigations. Since the criminals are using cyberspace to commit fraud and ultimately need to monetize that information and launder the proceeds to make them appear legitimate, it makes business sense to bring these functions together.

Regulators in some countries expect firms to have a holistic view of risk across functions and to report cyber events as part of normal AML and Suspicious Activity Report (SAR) obligations. With this model, financial institutions can also reap the benefit of reducing operational costs and enhancing efficiency while developing a cross-functional view.

> *By converging fraud, anti-money laundering (AML) and cybersecurity, financial institutions can consolidate data across historically isolated functions.*

WHAT DOES A HOLISTIC STRATEGY LOOK LIKE?

A holistic strategy is embedded in the culture of the financial institution—not treated as a project, but built into the DNA. This kind of strategy is risk-based and looks at all of the access points, including hardware, software, people, processes and content. It is a dynamic, continually evolving combination of prevention, detection, analysis and response that enables financial institutions to combat advanced threats and potential losses.

With a holistic approach that uses past events and creative thinking to identify problems before they occur, financial institutions can collaboratively collect and analyze intelligence from across the organization. This model improves intelligence-sharing across the industry and allows financial institutions to participate in exercises or drills that can continually test and improve security playbooks.

While it is important to examine each point in the banking relationship and each transaction, the most effective place to begin is the onboarding process.

Streamlining onboarding by leveraging modern technologies enables financial institutions to filter out suspicious and fraudulent actors and deliver a more frictionless experience to good clients.

Using a combination of technologies, including artificial intelligence (AI), RPA and NLP, financial institutions can ingest and process both structured and unstructured documents, minimize manual steps and reduce the need for making redundant requests of the client. Establishing an effective client onboarding process not only enables faster detection of potential fraud, it plays a significant role in developing strong and long-lasting relationships with new clients.

A holistic strategy also provides the visibility necessary to better prepare for auditing and compliance requirements. It improves efficiency, protects the brand and reputation, and protects against sanctions or fines. There is greater protection against identity theft and fraud from a customer perspective and fewer security incidents increase uptime, allowing customers seamless access to their financial lives.

HOLISTIC APPROACH USING MODERN TECHNOLOGIES

There are a host of benefits that come when a financial institution achieves a holistic fraud prevention strategy. Of course, the most significant and crucial benefit is financial—mitigating those massive potential losses, which, according to EY, are estimated at $1.4 trillion to $3.5 trillion each year.

Improving organizational visibility and reducing manual effort via AI, RPA and NLP can also free up security practitioners to focus on protection and mitigation, rather than compiling data from multiple sources and creating roll-up reports.

Reimagining risk through this lens requires more than technology investment. As stated before, people, processes and content all play a part in the successful implementation of a holistic approach. At the board level, a priority must be placed on financial crime operations, which includes dedication to providing sufficient human and technological resources.

Top management will soon be convinced that this approach not only ensures a robust defense against the most difficult attacks financial institutions encounter, but that enhancing customer experience, generating revenue and mitigating financial crime risk are complementary endeavors, and each strengthens the other.

Cheryl Chiodi is solutions marketing manager for financial services at ABBYY, a global digital intelligence company based in Milpitas, California.