Point of View

Five Tech Trends That Can Transform How Financial Institutions Detect and Prevent Financial Crime

As financial institutions expand their digital services to meet increasing demands from consumers and adjust to changing market infrastructure, financial criminals also are adapting to the changing paradigm. Criminals are developing new and innovative ways to infiltrate financial systems, and older technologies that mitigate fraud no longer work as effectively.

The risk of crime grows as financial institutions adopt online banking, international transactions, new payment systems and other technologies. Those global financial changes – and the threat from financial criminals – have driven the need for more effective solutions to mitigate fraud and money laundering in real time. Fortunately, more advanced technologies hold great potential for real-time mitigation.

Here are five trends to watch:

1) Artificial Intelligence and Machine Learning

Artificial intelligence is rooted in computer systems performing tasks that normally require human intelligence, such as visual perception, speech recognition and decision making. Machine learning is a subset of AI in which systems learn when exposed to new data rather than being programmed to perform a specific function.

AI technologies have been at work in financial services for some time and are rapidly evolving the customer experience and the back office. Robotic process automation can mimic the actions of people completing various types of processes, such as managing the steps in the maturation of a consumer's vehicle lease. Another evolutionary technology is the virtualized agent, which acts as a human avatar that has parsed a huge knowledge base. That can create a platform for lending systems, enabling financial institutions to employ digital labor as help desk attendants or loan officers, providing the steps to process a request while remaining compliant.

Machine learning can involve identifying patterns of behavior from large data sources (such as transaction-level data), so its application in financial crime detection and prevention means a shift from discovering fraud and money laundering based on selected data sources and limited rules to a more comprehensive and continuous monitoring of data and behavior that identifies pattern deviations.

Critically, machine learning can more rapidly identify predictive variables and convert them into detection models. The models can even take behavioral analysis to the individual consumer level, improving detection and false-positive rates while enabling regulatory compliance.

Machine learning can help the financial institution detect potential fraud and money laundering earlier – in real time – and more accurately. The resulting reduction in false positives and increase in prevention can improve customer satisfaction and retention. The automation will also enable financial institutions to deploy employees across higher value tasks.

2) Blockchain

Blockchain is a network that lets participants transfer ownership of digital assets and then records those transactions on a ledger in real, or near real, time. All of the participants have access to the ledger, making it a single source of truth for all transactions. Blockchain is prompting many organizations to consider how the technology can reform the current processes and procedures around authentication, integrity and security of data.

Blockchain enhances security by ensuring all parties are recorded, all transactions are cryptographically verifiable and no private data ever leaves the institution.

Today's financial service organizations often are the record-keepers for transactions such as security trades, loans and payments, so the implications of blockchain are far-reaching. Pick a service that involves moving assets, and it is likely blockchain has the potential to play a role. It could transform person-to-person payments, data sharing, person-to-business money transfers, securities exchanges or even movement of frequent-flyer miles, to name a few. The security features work toward enhancing confidence in the network and driving cost benefits in areas such as exchanges. The real-time functionality may lead to shorter, and less costly, settlement cycles on trade day.

The high level of security provided by blockchain has obvious implications for mitigating financial crime in real-time payments and preventing identity data breaches. When all parties are recorded, all information is accessible to those with access to the ledger, and the ledger enables real-time validation. It becomes much more difficult to carry out financial crimes.

3) Biometrics

Biometrics – the measurement and analysis of unique physical or behavioral characteristics, especially as a means of verifying personal identity – is both old and new. Identifying people through fingerprints to solve crimes has been around since the late 1800s. But in the past five years, advancement and adoption of the technology has skyrocketed. Apple's Touch ID and face unlock on Microsoft's Surface are bringing biometrics into the mainstream.

Some applications of the technology in financial services include biometric ID used by mobile banking applications, credit card "selfie" facial recognition to approve mobile payments and voice authentication in call centers where users can begin speaking to be transparently authenticated. Palm vein authentication uses biometric technology to scan the vein pattern of the palm. Authentication is unobtrusive and reduces risk by presenting information to tellers and service representatives – quickly, consistently and accurately – before the financial transaction gets underway. That enables tellers to easily spot fraud while efficiently fulfilling requests and completing transactions.

Biometric authentication relies on a mathematical representation of physical attributes that would be very challenging to re-create to allow unauthorized access. In particular, biometric authentication can make it easier to prevent fraudulent activity early in an interaction, reducing both fraud-loss money and operational costs of managing fraud downstream throughout a specified transaction.

As the technology becomes more widespread, additional multilayered fraud mitigation approaches could include mobile device facial recognition policies for high-value wire transfers, or combinations of biometrics, such as requiring both a voice print and facial recognition, for high-profile customers. Biometrics could even replace passwords; iPhone X with FaceID has done just that.

4) Predictive Analytics (Hybrid Model)

Predictive analytics turns data into valuable, actionable information used to determine the probable outcome of an event or the likelihood of a situation occurring. While predictive analytics is in use today, it is also evolving. Predictive models that are not trained on new fraud and money laundering techniques do not provide financial institutions the ability to rapidly respond to new attacks.

However, hybrid models have the flexibility to adapt to new conditions because they combine big data, sophisticated analytics and business-user expertise. Hybrid analytics can help financial institutions better detect, prevent and mitigate financial crime in real time.

The hybrid model often analyzes particular customer/transaction information from the financial institution against a broader set of consortium data. While data on its own can be useful, analytics transforms that data into actionable information so patterns emerge that can be used to predict, detect and prevent fraudulent behavior. The hybrid analytics model incorporates multiple predictive techniques and multiple patterns to build the best model possible for detecting financial crime. Finally, hybrid analytics models are purpose-built to let the business experts within risk departments influence the model.

Future applications could create super-hybrid models in which individual financial institutions could link to country-level or global-level information in a secure cloud environment. Those include:

- A global/country-level shared database with:
  - Known watch-list individuals/organizations
  - Blacklist information
  - Key analysis content for member financial institutions
- Financial institution-level databases with:
  - High-risk customers/businesses
  - Customer beneficial ownership structures and relationships
- A secured shared network or platform with:
  - Detection scenarios
  - Peer group calculations

Hybrid analytics could also be combined with machine learning and other advanced technologies to provide even more accurate financial crime detection and prevention.

5) Application Programming Interface

APIs have been used by IT teams for years to connect applications for the purpose of sharing data and functionality. But the increasing need to connect web apps with mobile apps, and mobile apps with each other, is placing greater importance on APIs.

Applications of APIs in financial services include: allowing corporate and consumer/retail customers and members to monitor accounts for specific events, such as large-dollar transactions posting to their accounts or the return of an item they originated; providing digital wallet and digital payment through web/mobile apps; and applying for and receiving an instant loan at the point of purchase. Through an API, companies can send payroll payments to employees in a variety of ways – to bank accounts, debit cards, social tokens including email addresses and phone numbers, and even paper checks. Immediate payment options mean payments can settle into recipient accounts in seconds.

An API layer can enable consumers to connect with financial institutions through various digital channels and would, in turn, enable financial institutions to connect with consumers and third-party vendors. APIs make integration faster, less costly and easier.

Leveraging APIs helps practitioners drive risk-based financial crime strategies that allow for nimble reactions to crime scenarios. The ability to selectively pull in client data and third-party data/tools enables financial organizations to snap in – and snap out – solutions for different business needs to balance financial crime mitigation, client experience and operational costs.

However, not all APIs are the same. Financial institutions are accustomed to providing solutions in a strictly regulated environment. Likewise, technology providers have years of expertise in ensuring customer data is kept secure and usable for the customer and

all banking products and services. Private or partner APIs conform to that use. However, open APIs in banking, as required by the European Payment Services Directive II, can present a higher level of risk for criminal activity and should be approached as part of a risk-based strategy.

Stay Ahead of the Curve

Financial institutions are trying to balance increased regulatory pressures with consumers' demands for new frictionless engagement channels and immediate access to funds. The solution for financial institutions lies in leveraging innovative anti-crime technologies to overcome the challenges they will face from ever-adapting fraudsters.

Factoring those technologies into an overall strategy can help financial institutions get ahead of the curve and gain an edge in an increasingly competitive fintech industry.

About the Author

Gasan Awad is the vice president of product management for financial crime and risk management at Fiserv. He has 20 years of experience in fraud and risk management in the traditional and emerging financial services sectors. He has executed innovative strategies and processes to mitigate fraud exposure, manage operational efficiency and enhance the customer experience.

Connect With Us

For more information about detecting and preventing financial crime, call 800-872-7882, email getsolutions@fiserv.com or visit www.fiserv.com.

Fiserv, Inc.
255 Fiserv Drive
Brookfield, WI 53045

800-872-7882
262-879-5322
getsolutions@fiserv.com
www.fiserv.com

51212-COL 00/17