

# New Solutions For New Threats

## AI: The Future of Financial Crime detection

### Table of Contents

- The Double-Edged Sword of Digitalization
- Legacy Solutions: A Weak Link in Detection
- Vulnerability of rules
- The Need for Speed
- Recent Developments in Regulations
- How AI Tackles Unpredictable Threats
- Advantages of AI
- Taking the Anti-Money Laundering Battle to the Cloud
- AI: Machine Learning Solutions for Digital Challenges
- AI for a Better Financial Future



## The Double-Edged Sword of Digitalization

Fintechs, payment service providers (PSPs), and even traditional financial institutions are leveraging technology to provide faster and more customer-focused options for money transfers and real-time cross-border and domestic payments, becoming more efficient, accessible and convenient.

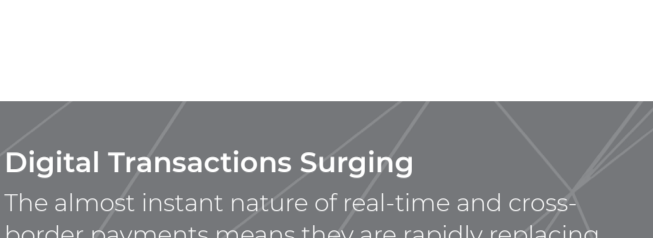
Yet, there are challenges and risks associated with digitization. With more financial transactions conducted online and emerging alternatives allowing anonymous and decentralized transactions, criminals are constantly evolving their techniques leaving traditional systems vulnerable.

Deploying advanced technologies like AI and machine learning on transaction monitoring, screening and client risk assessment is becoming increasingly important for financial institutions to stay ahead of bad actors and remain regulatory compliant.

### Digitalization Fuels Financial Crime

Digitalization has sparked an increase in the volume, velocity, and scope of economic crimes.

All forms of cybercrimes including ransomware, phishing, and mobile malware attacks have heightened in recent years. The financial industry is 300 times more vulnerable to cyber-attacks than any other industry.



**88%**  
Fintechs are Winning Ground

The fintech sector continues to expand at pace, with 46% of consumers exclusively using digital channels for their financial needs. While 88% of incumbent financial institutions believe that part of their business will be lost to standalone Fintech companies in the next five years.

**Digital Transactions Surging**

The almost instant nature of real-time and cross-border payments means they are rapidly replacing traditional methods. 80% of merchants, retail banks, and billing organizations favor real-time payments and open banking. **The transaction value of B2B cross-border payment is expected to exceed \$42.7 trillion in 2026.**

**\$42.7t**

## Legacy Solutions: A Weak Link in Detection

Legacy transaction monitoring methods typically rely on rules based methodologies and manual investigative processes which are less reliable and comprehensive than AI and machine learning. Accurate indications of financial crime are discovered by chance and not by the current systems in place. Upon discovering a new type of financial crime, it can take 6 to 12 months to re-program these systems to detect them. By then, criminals have likely devised new methods rendering the tool redundant once more.

**In a market where the amount of data to analyze has exploded:**

Financial criminals are innovative and consistently on the attack

Regulation/compliance is increasingly demanding and complex

Rules are outdated as criminals plot new schemes, and reprogramming can't keep up with emerging financial services.

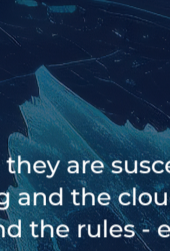
Despite decades and billions of dollars of investment, over 95 percent of alerts generated by legacy monitoring and screening technologies are "false positives."



**95%**  
Rules-based: **95% false positives**



**28%**  
Artificial Intelligence (AI)/Machine Learning (ML): **28% false positives**



**1%**  
Semi-supervised AI/ML: **1% false positives**

### Vulnerability of rules

Rules-based systems have another major vulnerability - they are susceptible to being outsmarted by bad actors. Cyber-criminals are constantly innovating and the cloud-based digital world makes it relatively easy for them to devise new ways to get around the rules - especially as the rules are fairly predictable.

When the rules change, the tools created around them no longer fit the purpose. Even the best rules-based anti-money laundering (AML) tools are unable to detect new criminal behaviors that were specifically designed to evade detection.

### The Need for Speed

Rules-based AML is particularly troublesome for fintechs whose business model is based on speed, agility, and efficiency. These rules-based AML systems often lack the flexibility to adapt to changing regulatory requirements and evolving money laundering techniques.

Fintechs need a solution that can shift and scale as fast as they do, adapt to new realities without the need for cumbersome programming, and reliably detect suspicious transactions with a reduced amount of false positives.

**15,000**  
hours spent each year on risk assessments GRX

**87%**  
of organizations have no additional capacity due to staffing issues

**Over \$2bn**  
in fines each of the last two years

## Recent developments in Regulations

- Regulators worldwide, including;
- › European Union (EU SAML and 6AMLD)
  - › Financial Conduct Authority (FCA)
  - › Financial Stability Board (FSB)
  - › Bank Secrecy Act (BSA),

and bodies such as the Financial Action Task Force (FATF) and regional equivalents, have heightened their focus on improving transparency, strengthening due diligence requirements, and implementing robust monitoring frameworks to combat AML and counter-terrorist financing (CFT).

Key developments include the proliferation of risk-based approaches tailored to individual jurisdictions' vulnerabilities, advancements in technology for transaction monitoring and customer identification, and expanded cooperation among international financial institutions. This period has also witnessed a notable trend towards more severe penalties for non-compliance, reflecting a growing consensus on the critical importance of AML/CFT measures in safeguarding the integrity of the global financial system.

FATF specifically acknowledges the transformative potential of new technologies in enhancing the efficiency and effectiveness of AML/CFT measures. The transition from outdated legacy AML/CFT compliance systems is a challenging yet essential step to augment human potential, particularly in light of criminals increasingly leveraging AI for illicit activities.



### The Status of Global Regulation

**Europe**  
The Artificial Intelligence Act was approved on March 2024

**UK:** AI Regulation White Paper was published by the UK government, setting out its proposed regulatory framework for AI (March 2023)

**North America**  
US: The Landmark Executive Order around AI was issued in 2023, including standards around AI safety and security, and the establishment of new cybersecurity programs to help fix vulnerabilities in software.

CANADA: In March 2023 the Digital Charter Implementation Act is the country's first attempt at AI regulation: "The Artificial Intelligence and Data Act (AIDA)".

**Latin America**  
MEXICO: The Law for the Ethical Regulation of Artificial Intelligence was introduced (March 2023), in process of approval.

BRAZIL: A new law seeking to regulate Artificial Intelligence will be evaluated in 2024.

**Asia**  
CHINA: Extensive AI regulations have been implemented, including governance of generative AI.

JAPAN: Released Draft AI Guidelines on December 2023 to be finalized during 2024.

SINGAPORE: Has taken a pragmatic approach and has no intention to set mandatory rules for AI yet.

**Australia:** Government working on generative AI

## How AI Tackles Unpredictable Threats

The increasing dominance of real-time payments and rising regulatory scrutiny pose a challenge for the financial industry to find effective solutions for transaction monitoring and sanctions screening. AI machine learning solutions provide the following advantages:

- › Handle high transaction volumes efficiently.
- › Detect complex patterns of suspicious activity.
- › Reduce false positives.
- › Adapt to regulatory changes without the need for re-programming.
- › Ensure data quality and integration.
- › Accommodate cross-border transactions and global operations.

Going forward, fintechs and PSPs must assure counterparty banks, regulators and customers across their payments landscape, they have the capability to detect potential financial crimes.

**A mere five years ago, few could have foreseen the near-total shift to cloud-based financial services, the burgeoning dominance of real-time digital payments, and the ascent of fintechs over traditional banks. Looking ahead, the next five years promise even more transformative changes in the financial landscape.**

Regulators are also acknowledging AI's potential for AML efforts, with FATF strongly advocating its use alongside machine learning for detecting both AML and CFT activities. According to a recent Deloitte report, RegTech is hailed as the future of banking, highlighting that "financial service providers are investing increasingly in intelligent solutions that use modern technologies to reduce the costs of regulatory compliance."

## Advantages of AI

**Independent of rules and static models** - analyzes a staggering array of factors within datasets, learning what is normal and spotting patterns and anomalies without relying on predetermined human rules, thresholds and suppositions.

**Detects "unknown-unknowns"** - derives conclusions from the data alone (not from rules programmed by developers), therefore it can identify patterns, connections or, "unknown-unknowns" - not detectable by humans.

**High detection-worthy & low false alerts** - higher accuracy and fewer false positives than rules-based systems. Financial Institutions using intuitive AI will need fewer resources to monitor the output of the system.

**Continuous improvement** - adapts itself to changing realities as it only needs the data set to detect the unusual events. Intuitive AI and machine learning systems continually improve in accuracy as they "learn" more about datasets.

**Fast, simple, low-cost integration** - there is no need to reprogram with new rules. Intuitive AI systems are faster, easier, and cheaper to onboard.

**Prioritize cases that need to be investigated** - the root cause of failure of traditional transaction monitoring derives from effort invested in redundant cases. While most alerts are meaningless they still require full investigations, thus financial institutions get side-tracked looking in the wrong direction. The new wave of AI-based transaction monitoring focuses resources and attention on meaningful detection.

## Taking the AML Battle to the Cloud

McKinsey research shows that by 2030, cloud technology will account for EBITDA in excess of \$1 trillion across the world's top 500 companies. It is also estimated that a shift to the cloud will lower the costs associated with technical violations in financial services firms by 26 percent. Similarly,

Deloitte, in a report on "Cloud Banking" identifies the cloud as a potential game-changer for financial services organizations will operate in the future. Cloud-based transactions rely on a secure environment in which to operate but, shifting data to the cloud introduces multiple vulnerabilities and exposes the data to potential attack by criminal entities.

In order to de-risk operations effectively and maintain compliance, the financial industry needs solutions that operate in the cloud where most of the transactions occur. Cloud-based AML and compliance services offer several advantages, including ease of deployment, rapid results, and increased scalability.



## AI: Machine Learning Solutions for Digital Challenges

A digital world needs digital solutions. Legacy rules-based systems simply can't catch up. According to the Digital Banking Report, 35% of financial organizations have deployed at least one machine learning solution. AI solutions being deployed by financial services firms in risk management, predictive analytics, customer engagement, and cybersecurity, are yielding impressive results on every front.

AI has the potential to improve the way the financial services industry tackles AML transaction monitoring, sanctions screening, and know your customer (KYC) checks, offering better customer experience, faster and more efficient transactions, and especially, more secure and stable services.

By creating a greater variety of secure and trusted channels for payments, AI will pave the way for even the more traditional and risk-averse financial institutions to create alternative payment routes and extend their own services -- independently or in partnership with PSPs or Fintech firms.

AI could save the banking industry more than \$1 trillion in projected cost savings by 2030. Over the next 12 years, traditional financial institutions could reduce their costs by 22 percent by applying AI to compliance, KYC and AML processes, as well as other forms of data processing.

**57%**  
of financial institutions have deployed or are planning to deploy an AI/ML solution



## AI for a Better Financial Future

AI has the potential to create a more inclusive financial global system. It could change the balance of power on the world stage, evening out gaps with the less-developed world.

Digitization provided the means for millions of people from developing countries to access formal financial services. Additionally, digital financial services can help improve people's income-earning potential, increase women's economic participation, and create more inclusive societies.

### About ThetaRay

ThetaRay is a pioneer in the field of anti-money laundering (AML) with AI-powered solutions that deliver trusted transactions and trusted customers for banks, fintechs, and regulators around the world.

Designed to reduce our clients risk exposure through unparalleled detection of financial crime, uncovering 'unknown-unknowns' and delivering insightful alerts, with a precise assessment of customer's risk profiles.

Fast to deploy, fast to update and fast to maintain, our solutions enable cost-efficient AML compliance.