FINANCIAL SERVICES | eBook

Banking on Intelligence:

How AI and ML Help Banks Stay Ahead of Cybercriminals and Compliance Regulations

ABBYY

Table of Contents

Where the Money Is

When famed American bank robber Willie Sutton was asked why he robbed banks, he replied, “That’s where the money is.”

Today, banks are still “where the money is,” but criminal techniques have come a long way from the armed robberies that Sutton was known for. Financial crime has gone digital, and cybercriminals are inventing new methods of fraud and money laundering as quickly as banks can implement countermeasures. Banking ranks first among industries in the annual cost of cyberattacks—more than $18.3 million per year per company.

The origins of know-your-customer (KYC) and anti–money laundering (AML) regulations go back to the Bank Secrecy Act of 1970 and were strengthened after the terrorist attacks of September 11, 2001. In the course of the investigation that followed, the U.S. Congress quickly discovered that the

IN APRIL 2020, A CYBERCRIMINAL GROUP KNOWN AS THE FLORENTINE BANKER GROUP LAUNCHED ATTACKS AGAINST LEADING ISRAELI AND UK FINANCIAL FIRMS, STEALING

$1.3 MILLION

IN JUST **FOUR SEPARATE TRANSACTIONS**.

Source

operation was funded using cybercrime and money laundering. For the first time, cybercrime was officially codified as terrorism and received special attention in formulating counter-terrorism measures, including Combating the Financing of Terrorism (CFT).

Complying with these regulations can be effective in preventing fraud and theft, yet banks must remain vigilant and take additional steps to keep pace with rapidly evolving cybercriminal methods. KYC and AML regulations also carry heavy fines for violations and create market and reputational risks, raising the stakes further for failing to implement adequate safeguards. As of December 2019, global penalties for KYC/AML non-compliance totaled $36 billion.

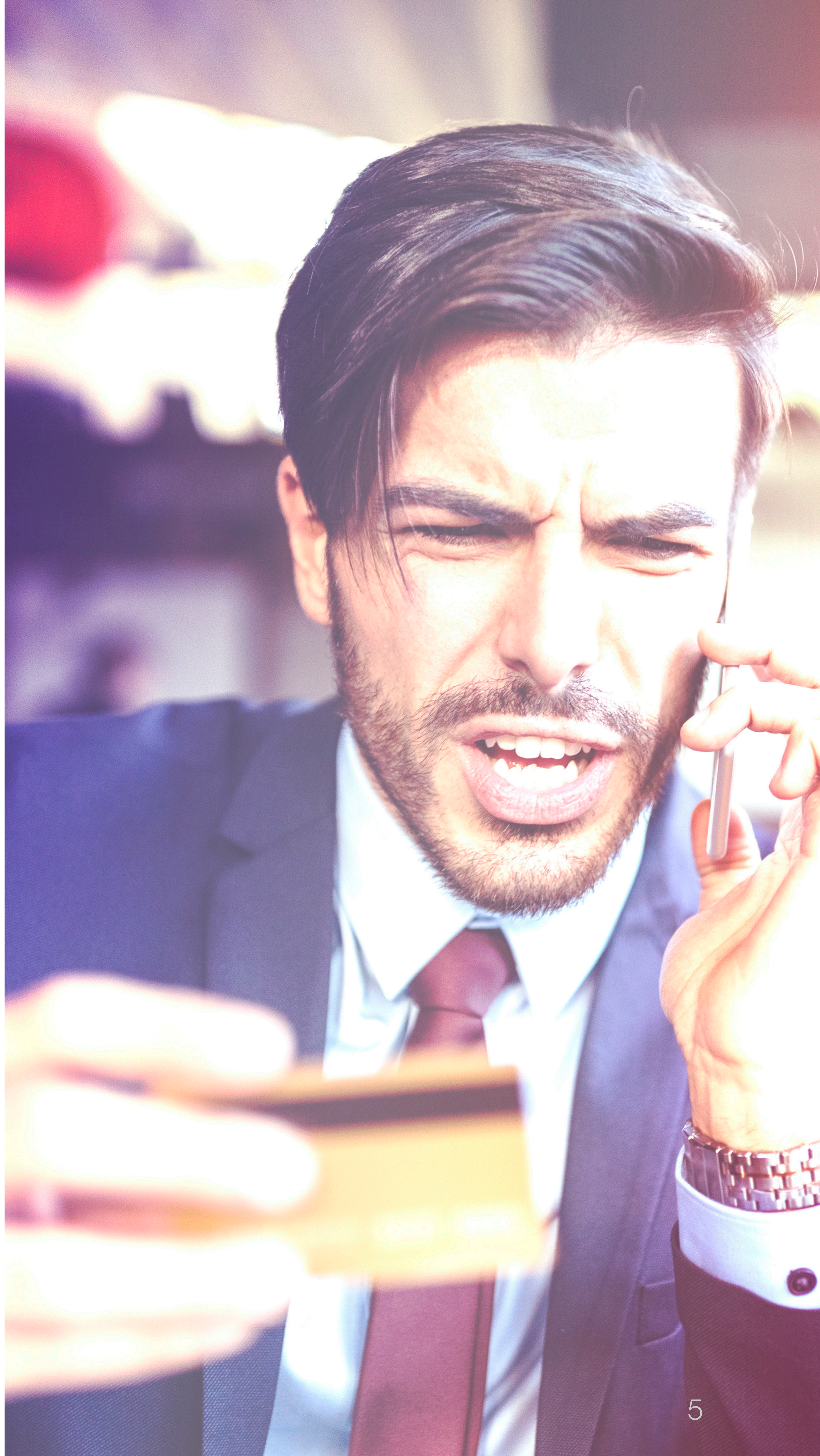
Preventing sophisticated crimes requires sophisticated measures. Fortunately, today's artificial-intelligence-driven technologies can provide banks with the visibility into their processes and their content that they need to align with KYC/AML/CFT regulations and be flexible to adapt as conditions change.

Financial Crimes Have Evolved

Driven by heightened competition and evolving customer expectations, financial institutions rely increasingly on automation, mobile technology, and contactless interactions, especially since the onset of the COVID-19 pandemic. While these measures deliver significant benefits in terms of productivity and customer satisfaction, they can also create new vulnerabilities that cybercriminals can—and do—exploit.

COVID-19 is also impacting abilities to implement anti-money laundering and counter terrorist financing (AML/CFT) obligations, from supervision, regulation, and policy reform to suspicious transaction reporting and international cooperation.

The increase in remote transactions has provided fertile ground for these nefarious actors, targeting populations who may be less familiar with online platforms and exploiting stimulus measures.



Fundraising for fake charities, fraudulent investment scams, increased phishing, and ransomeware attacks increased physical cash transactions. When the market stabilizes, large movements to re-deposit funds could provide cover to efforts at laundering illicit funds. COVID-19 has also created a pause in new AML/CFT policy and legislatives initiatives.

Today's perpetrators of financial crimes have figured out how to leverage an institution's own systems and processes as mechanisms for laundering and stealing money, such as

1. **Virtualization:** System and application vulnerabilities can be exploited to allow unauthorized access to account data.
2. **Process automation:** Criminals can uncover loopholes in automated processes that automated reviews might miss.
3. **Customer identification:** Identification used to identify customers can be stolen to commit identity theft.
4. **Customer onboarding:** Cybercrime perpetrators can create synthetic accounts using fake customer identities.

THE AMOUNT OF MONEY LAUNDERED GLOBALLY EACH YEAR IS ESTIMATED BETWEEN

$800 BILLION AND $2 TRILLION,

ROUGHLY

2–5% OF GLOBAL GDP.

Source

ONCE THE ASSOCIATED COSTS ARE ACCOUNTED FOR, FINANCIAL INSTITUTIONS **LOSE THREE DOLLARS FOR EVERY DOLLAR LOST DIRECTLY TO FRAUD.**

Source

How can financial institutions counteract this constant flow of attacks? Manual oversight can be helpful, but is inherently limited by

- Human employees’ inability to keep pace with the volume and speed of transactions on a 24/7 basis, combined with inadequate controls over transaction monitoring and reporting
- The increased risk of human error
- The challenge of keeping human employees informed on the latest criminal techniques
- The risk of human employees engaging in financial crimes themselves

The Compliance Angle: Meeting KYC and AML/CFT Requirements

To align with KYC and AML regulations, financial institutions must demonstrate that they have procedures in place to detect and take action on criminal activity, including verifying the identities of customers and the authenticity of transactions.

While many banks have verification processes and systems of record in place for their structured data, the large amount of customer data that originates in documents is creating a broad area of vulnerability for them. They are missing the link that would tie their data architectures to the documents where a large portion of customer and transaction behavior—and insights about that behavior—originate.

One instance in which this document-based data can lead to compliance issues is the requirement to track chain of custody. Chain of custody refers to the practice of tracking the lifecycle of data from the point it enters the organization until the day of its destruction or warehousing. A compliant chain-of-custody record can answer such questions as where in the organization the data originated, where it has gone, who has touched it, and what, if any, alterations have been made to it.

Documents are essential business records and must maintain their integrity throughout the chain of custody; if any alterations are made, they must be noted. In the case of documents, tracking the chain of custody can be problematic for three equally important reasons:

- Incomplete understanding of the documents themselves
- Incomplete understanding of the processes the documents go through
- Insufficient visibility into who has interacted with the documents

Example: Customer Onboarding

If a customer submits a driver's license as part of the onboarding process, a chain-of-custody record should incorporate when and how the document was scanned, how the data was extracted and verified, what happened to the scanned image after onboarding, and how the extracted data can be traced back to the document. Any gaps in this chain could result not only in KYC compliance violations, but also in vulnerabilities that could be exploited by cybercriminals. Customer onboarding—where the bank first establishes the identity of the customer via documents—is the critical first step to get right in ensuring KYC compliance.

IN 2017 ALONE, BANKS SPENT APPROXIMATELY

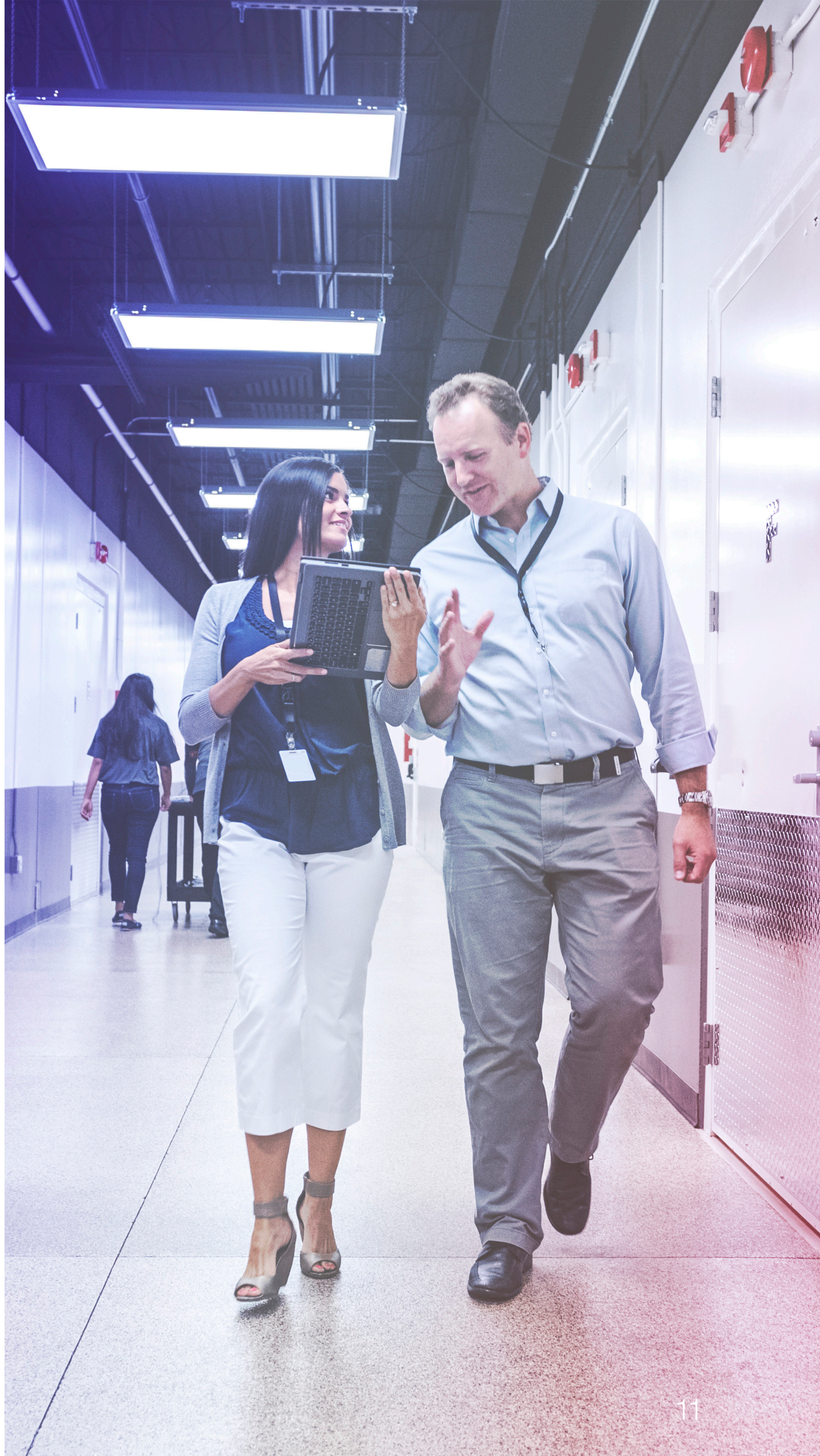
$8.2 BILLION

ON ANTI–MONEY LAUNDERING (AML) CONTROLS.

Source

Staying Ahead with Digital Intelligence

To address the dual challenge of complying with KYC/AML/CFT regulations and forestalling criminal activities that may fall outside compliance requirements, financial institutions need a multi-front battle plan that addresses people, processes, and documents. First, they must have a means of scrutinizing documents to detect attempted fraud. Second, they need visibility into their processes that enables continuous monitoring for irregularities that could indicate fraudulent behaviors. Third, they need insight into the ways that people are interacting with the processes and the documents that could indicate suspicious behavior. This approach will arm banks with the Digital Intelligence needed to protect their institutions both from fraud and from regulatory violations.



Digital Intelligence is a new approach to using the latest artificial intelligence (AI) and machine learning (ML) technologies to deliver key capabilities that provide banks with confidence in document chain of custody:

- Validation of customer onboarding documents—both structured and unstructured—and their content at the point of entry
- Intelligent extraction of content from those documents that can be validated and/or flagged as suspicious
- Process discovery that reveals patterns of suspicious behavior between people and documents and gaps in processes that can create vulnerabilities for attack

When applied to fraud prevention, Digital Intelligence offers financial institutions the tools they need to meet compliance requirements and stay ahead of criminals while avoiding the pitfalls of manual approaches that cannot keep pace with or scale to meet the challenge.

Document Integrity

Even as the financial industry progresses toward digital transformation, much of a bank's customer data originates in documents: forms of identification, corporate evidence of formation, loan applications, tax returns…the list goes on. If financial institutions are to prevent fraud and meet their compliance obligations, they must have a reliable way of examining each customer document for irregularities that could signal criminal intent. They also must provide a direct link between their systems of record for KYC/AML compliance and their customer interactions from onboarding through entire customer journeys.

Document integrity plays a vital role in the chain-of-custody monitoring and documentation that is critical to KYC/AML compliance (see "The Compliance Angle"). By validating documents and their content during the onboarding process, banks are able to track customer data from the point where it entered the organization (customer onboarding) through the complete lifecycle, all the way to off-boarding. Should a compliance officer request chain-of-custody documentation, the financial institution can account for every touchpoint.

Process Integrity

As soon as customer data enters a financial institution, whether through documents or from digital sources, it becomes fodder for any number of processes, including customer onboarding, compliance checks, loan approvals, and many more. While most banks may have a good idea of how these processes should execute, the gaps between theory and practice may be broader than they think—and those gaps could present opportunities for fraud or data theft.

Process discovery uses data from digital and physical sources to give banks visibility into how their processes actually execute from beginning to end. By gathering and analyzing the timestamp data generated by information systems, Process Intelligence uses advanced algorithms to create a "digital twin" of business operations and processes. These visual models offer detailed insights into how processes actually execute on a day-to-day basis—both the "standard" or "ideal" path and all variations.

In the drive to prevent fraud and money laundering, process monitoring can uncover irregularities in data handling that could be exploited by cybercriminals. It can also monitor processes 24/7 for potential security vulnerabilities and automatically alert process owners for immediate intervention.

As discussed above, tracking the chain of custody, with its documents and data, is a vital component of KYC/AML compliance. By automatically mapping process execution, banks can track the lifecycle of customer and transaction data as it moves through and between processes with their essential documents and, if required, provide accurate documentation of the chain of custody.

Continuous Learning

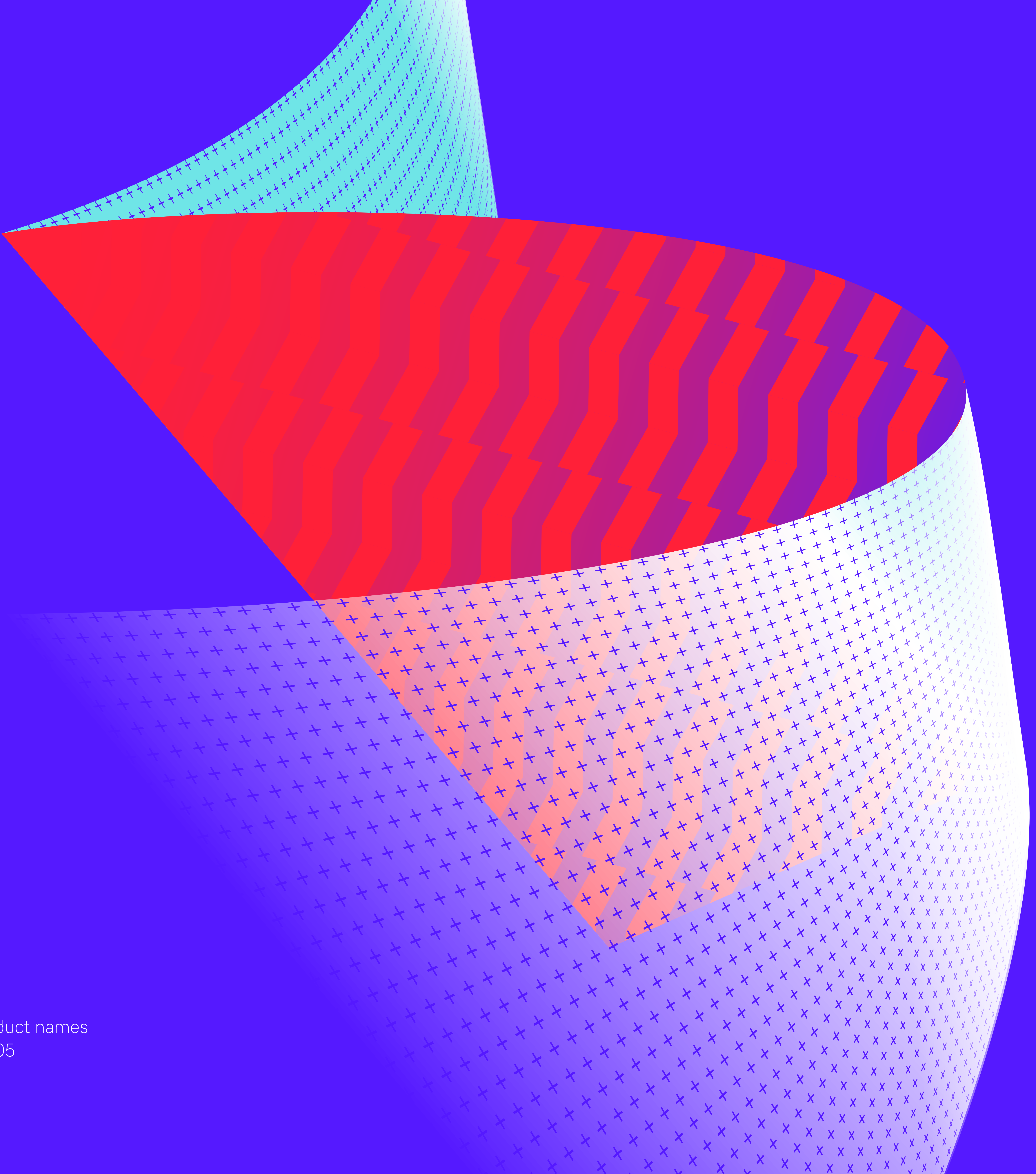
Compliance and fraud prevention are in a continuous state of flux, as new regulations emerge and as criminals invent new approaches to perpetrating fraud. Digital Intelligence solutions are highly adaptable as conditions evolve and compliance regulations and guidelines change. ML technology is employed to enable these solutions to learn from each iteration and adapt accordingly.

Looking Ahead

As banks and other financial institutions progress toward digital transformation, sometimes the side effects of that progress can lead to less-than-favorable results. Today's cybercriminals have figured out how to use an organization's own digital infrastructure to perpetrate fraud and data theft, and staying ahead of them requires using all tools available.

AI-driven solutions can automatically review and monitor hundreds of processes and thousands of documents, quickly and accurately, to flag signs of possible criminal activity. AI will not replace human compliance and fraud prevention experts; on the contrary, it can be a game-changing asset that frees employees from routine oversight tasks and enables them to focus on more complex problems. The combination of human expertise with a digital workforce to help financial institutions scale and adapt quickly creates a unique advantage in the battle against financial crime, enabling banks to comply with KYC/AML regulations while fortifying their own defenses against cybercrime—today, tomorrow, and for years into the future.

ABBYY



For more information visit:
www.ABBYY.com/finserv

Contact our offices worldwide:
www.ABBYY.com/contacts