Fighting financial crime with AI

How cognitive solutions are changing the way institutions manage AML compliance, fraud and conduct surveillance

IBM

Highlights

- Fraud and compliance challenges are reaching a critical point
- Regulators and financial institutions are changing their views of artificial intelligence (AI)
- Top financial crime AI use cases
- IBM point of view: Financial institutions are gaining value from cognitive
- Checklist for the AI journey
- Next steps: Why act on AI now?

Challenges from financial crime incidents and penalties grow

If the frequency of high-profile financial crime incidents and amount of losses and regulatory penalties are any indication, financial institutions across the globe are dealing with systemic threats when it comes to financial crime. From fraud and money laundering to know your customer (KYC) and insider trading, these offenses can have a significant impact not only on organizations, but also on individuals and economies. They can fuel criminal enterprises and activities, including human trafficking, terrorism and drug trade.

Contrary to popular belief that governments are in a period of deregulation, penalties from the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury alone have risen dramatically. In the first five months of 2019 alone, penalties have been higher than the last four years combined, with approximately USD 1,228 million versus 812 million.[1] In 2017, it was predicted that fines for misconduct were expected to exceed USD 400 billion by year 2020.[2] However, with major recent incidents, such as the Troika Laundromat money laundering scandal,[3] that estimate may increase.

Economic sanctions have been used as political weapons since ancient times. Today, the United States, the European Union (EU) and other developed economies increasingly use sanctions to support their policies.[4] Yet sanctions can fuel demand for black markets, which increases the risk of costly penalties for financial institutions that are targeted by criminals moving illicit funds.

Lists of sanctioned individuals are extensive and growing rapidly. The current US list alone runs over 1,200 pages.[5] These increases mean that firms need to continually strengthen and update their KYC due-diligence processes and controls.

Sophisticated criminal groups continue to take advantage of new technologies and fast-changing conditions to carry out increasingly complex and massive illegal schemes, from hiding illegal funds to various forms of first-party and third-party fraud. The net result is that financial institutions face more crime threat than ever, from inside and outside their organizations.

As part of their mandated compliance and fraud prevention programs, financial institutions will have a variety of systems and technologies in place. But with complex and ever-changing fraud and financial crime patterns, these tools lack the ability to quickly and effectively stop these incidents.

To remedy this technical failing, financial service organizations have been increasing the amount of human capital to triage anti-money laundering (AML) alerts, investigate potential fraud and monitor for conduct infractions.

However, as transaction levels continue to rise, so will the number of analysts and investigators required to sustain adequate standards. This situation leads to higher costs, but without a corresponding increase in return.

What are the main challenges you face during the investigation process?

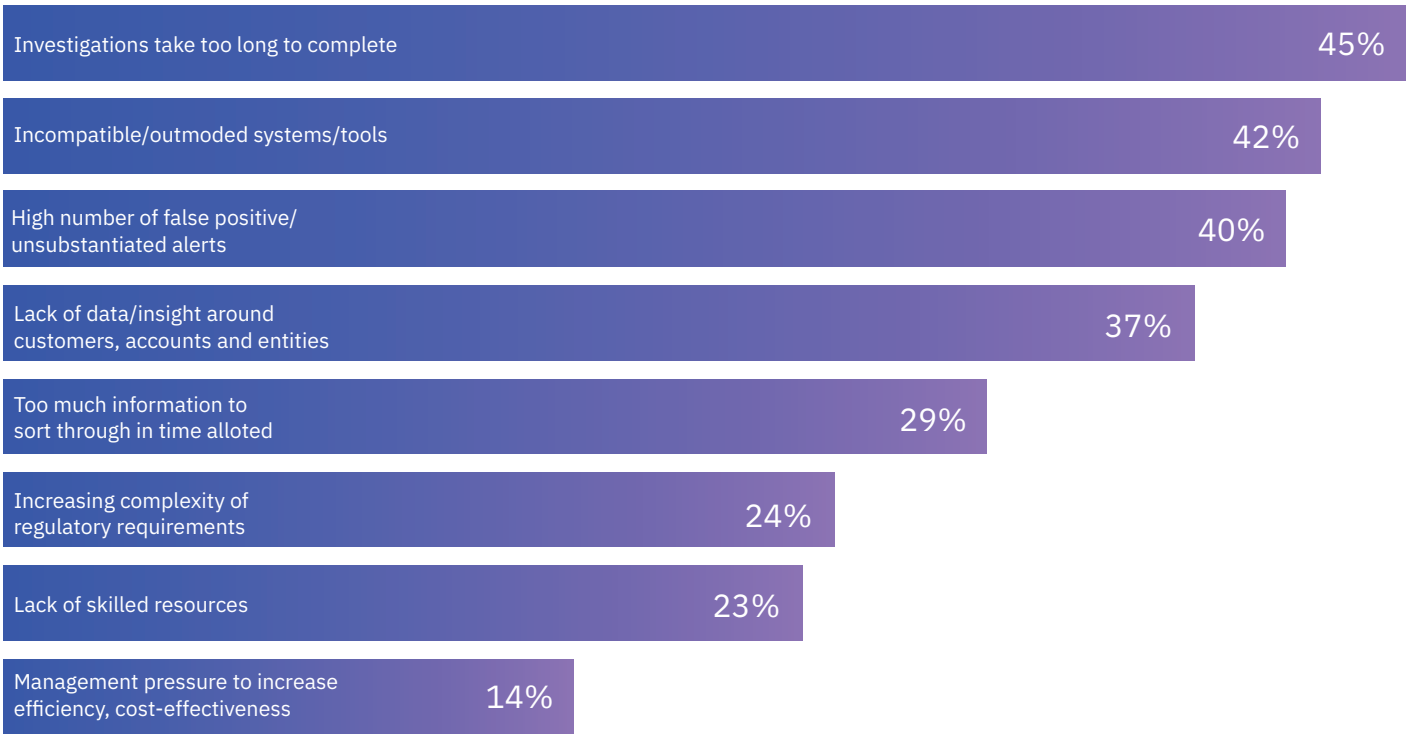

Figure 1: Risk.net Survey Report "Smarter thinking around financial crime prevention", January 2019

Financial institutions and regulators support AI and machine learning

Other dynamics that create new risks from financial crime include disruptive technologies, the growth of new financial services products and channels, and the explosion of payments and transaction volumes. These changes all create situations for financial organizations that can be manipulated by internal or external bad actors. But new technologies can also provide much needed relief, as well. Understanding that the status quo of adding resources to keep up with financial crime management demands is no longer sufficient, regulators have been changing their stance toward advanced technologies.

In December of 2018, five US government agencies, including the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), Financial Crimes Enforcement Network (FinCEN), National Credit Union Administration and Office of the Comptroller of the Currency (OCC), issued the Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing. The document encourages banks to implement innovative approaches, specifically referencing AI. In this statement, the agencies even mention that these approaches "can maximize utilization of banks' [Bank Secrecy Act] BSA/AML compliance resources."[6]

Regulatory encouragement is also seen from the Australian Transaction Reports and Analysis Centre (AUSTRAC), which launched an initiative to facilitate collaboration across the Australian banks that includes the application of advanced analytics to improve the investigation of suspicious activities. Plus, the UK Financial Conduct Authority (FCA) [7] has held multiple public workshops, bringing together FinTech's and established financial institutions to experiment with various new technologies that improve the identification and management of potential financial crimes.

Given this measured, but encouraging approval from regulators, financial services organizations are exploring ways to limit disruptive reinventions. They seek to augment and alleviate the time-consuming, labor-intensive and often inaccurate processes that encompass their financial crime operations.

The key areas where AI and cognitive solutions are having the greatest impact so far are transaction monitoring and sanctions screening alert triage, due diligence reviews, payment fraud modeling, and conduct surveillance investigations. The five use case studies in this paper demonstrate how AI, machine learning (ML) and robotic processing automation (RPA) are key technologies to cost-efficiently resolve the technical and process gaps that criminals exploit today.

Definitions

Artificial intelligence (AI)	AI makes machines act more intelligently. It includes basic and applied research in ML, deep question answering, search and planning, and cognitive architecture.
Cognitive computing	Cognitive systems learn at scale, reason and interact with humans naturally. Self-teaching algorithms use data mining, visual recognition and natural language processing (NLP) so that the computer is able to solve problems and thereby optimize human processes.
Machine learning (ML)	ML uses algorithms that learn from data and create foresights based on this data. It gives computers the ability to keep learning without being reprogrammed.
Robotic processing automation (RPA)	RPA solutions mimic the actions of human users to perform repetitive and high-volume tasks, freeing people to focus on higher-value tasks.

1. Use case:

AI reduces AML noise with smarter alert triage

Within financial institutions, it's not uncommon to have high false-positive rates that is, notifications of potential suspicious activity that do not result in the filing of a suspicious activity or suspicious transaction report, well above 90 percent. In fact, for AML alerts, high false positives are the norm. The reason for this is a combination of dated technology and incomplete and inaccurate data.

Traditional detection systems provide inaccurate results due to outdated rules or thresholds, or peer groups creating static segmentations of customer types based on limited demographic details. Also, account data within the institution can be fragmented, incomplete and housed in multiple locations. These factors are part of the reason why alerts and AML are key areas to apply AI, advanced analytics and RPA. The technologies can gather greater insight, understand transactional patterns across a larger scale and eliminate tedious aspects of the investigation that are time-consuming and low value. In short, AI can augment the investigation process and provide the analyst with the most likely results, driving faster and more informed decisions with less effort.

Which areas of the AML and CDD investigation process do you believe could be improved using artificial intelligence/cognitive capabilities?

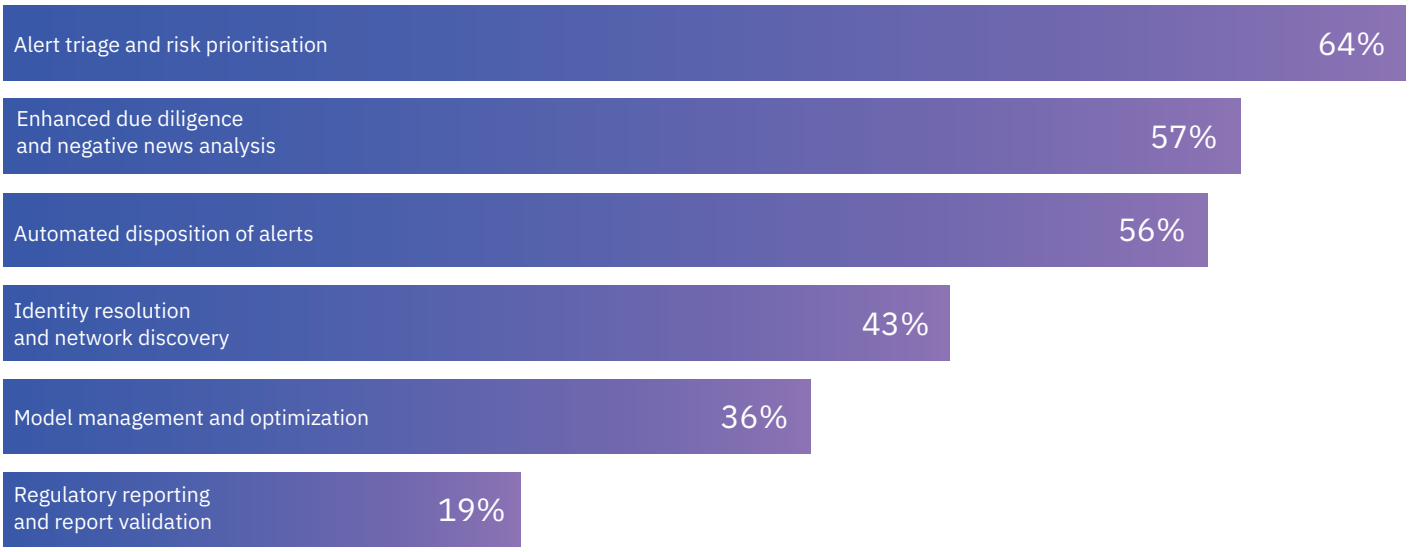

Figure 2: Risk.net Survey Report "Smarter thinking around financial crime prevention," January 2019

Customer case study

Top 10 global bank speeds AML investigations 200 percent

Business challenge

This multinational financial institution was dealing with a typical challenge in their approach to AML compliance. It had existing transaction monitoring systems that were producing an unwieldy number of alerts. In addition, after several mergers with and acquisitions of other financial institutions, the firm had a patchwork of data sources. There was little insight into whether a single customer appeared in multiple systems as an account holder in legacy institutions. As a result, AML analysts spent much of their time data gathering and attempting to corroborate alerts that resulted in 99 percent false-positive outcomes.

At this point, the institution leveraged IBM® Financial Crimes Insight to reduce the time and effort spent on data gathering, improve prioritization of the highest risk alerts and speed decision-making by providing analysts with better insight on customer risk.

Transformation

- **Analyze existing alerts:** As a first step, IBM reviewed the last 12 months of AML alerts to uncover areas of improvement. From the output, it was discovered that 7 percent of the alerts were duplicates, a result of the inconsistent data sources at the bank.
- **Understand fragmented data:** Next, IBM assessed 1.7 million customer records against eight key fields to determine if necessary information was present and being pulled from the correct source systems. The result showed that only 52 percent of the records were deemed "healthy", meaning all necessary information was present and accurate from source systems. As a result of the health check, potentially 1.6 million false hits can be avoided by addressing these discrepancies.
- **Speed investigations with context:** Lastly, to help the bank increase the speed and accuracy of complex sanctions and transaction monitoring investigations, IBM found ways to gather and combine data to help the analyst make better decisions faster. By per-aggregating data, such as related alerts, cases and Suspicious Activity Reports (SARs); comparing a subject's KYC profile against the subject's actual profile; and analyzing negative news related to the entity, the analyst is provided with the right information to make a more informed decision.

Results

- **A 50 percent reduction in alerts:** Lowered false positives from the existing AML transaction monitoring system by applying additional layers of advanced analytics
- **A 200 percent faster reviews:** Increased investigation efficiency by using relationship analysis and text mining to automatically collect data

Business impact

- **Improves use of limited resources:** By providing greater insight and eliminating duplicates, analysts can focus on the truly suspicious behaviors and quickly resolve low-risk alerts.
- **Increases customer visibility:** With a consolidated view of customer accounts, the bank has improved its understanding of customer behavior and risk.
- **Speeds response to emerging risks:** By proactively collecting and presenting contextual information to analysts, risks can be prioritized and resolved more quickly.

Customer case study

Large UK bank lowers false positives 70 percent

Business challenge

A large financial institution based in the United Kingdom was dealing with a triple threat of AML inefficiency. First, its AML transaction monitoring system was generating 99 percent false-positive alerts, leading to wasted analyst effort. Second, the firm had multiple data sources across multiple lines of business with inconsistent data, leading to lengthy reviews to understand which data was accurate and which was outdated. And third, compounded by the prior points, it incurred high costs to conduct customer list screening across its large customer base.

The bank looked to IBM Financial Crimes Insight to streamline its AML investigations and better understand where its process could be improved.

Transformation

- **Start with the data:** Over a two-week period, IBM connected to the bank's disparate data sources across multiple lines of businesses. From this consolidation effort, subsequent analysis provided insight into previously unknown relationships and behaviors.
- **Identify entities and networks:** With this combined data set, IBM found more than 20,000 alerts that were connected with entities that had more than one customer ID. In addition, by better understanding individuals, previously hidden relationship networks were exposed, providing not only fewer false positives, but fewer false negatives, as well.
- **Improve accuracy and outcomes:** Lastly, using ML and statistical models, IBM scored alerts based on past dispositions to improve risk prioritization and eliminated time wasted on low-risk investigations. Using this priority ranking, the highest risks were sent directly to senior investigators.

Results

- **There were 70 percent fewer false positives:** Eliminated false-positive alerts using a combination of strategies to better understand individuals, as well as underlying risk
- **There were 50 percent less false negatives:** Improved accuracy and reduced overlooked risks by better understanding connections between entities and relationship networks

Business impact

- **Improved use of limited resources:** By providing greater insight and eliminating duplicates, analysts can focus on the truly suspicious behaviors and quickly resolve low-risk alerts.
- **Increased customer visibility:** With a consolidated view of customer accounts, the bank has improved its understanding of customer behavior and risk.
- **Faster responses to emerging risks:** By proactively collecting and presenting contextual information to analysts, risks can be prioritized and resolved more quickly.

2. Use case:

AI speeds entity research for intelligent customer insights

As part of a financial service organization's risk management process, periodic reviews of customer accounts are performed to ensure the institution isn't unwittingly being used for illegal activities. As a practice, accounts and individuals that represent a higher risk undergo these reviews more often than lower-risk entities.

For these higher-risk accounts, additional scrutiny is performed in the form of enhanced due diligence (EDD). This process involves not only looking at government and public watch-list and sanctions lists, but also news outlets and business registers to uncover any underlying risks. As one would think, such less-common investigations took the majority of the due diligence process because they typically required lengthy, manual searches and validation that a name was the individual or entity under review.

With modern technologies like entity link analysis to identify connections between entities based on shared criteria, as well as NLP to gain context from structured and unstructured text, much of this investigation process can be automated. In addition, by using AI to perform the initial search and review of a large number of articles and information sources, financial institutions gain greater consistency and the ability to record the research results and methodology.

Much like the AML alert triage example previously mentioned, the key is not to automates analysts from the process. Instead, AI automates the data gathering and initial review to focus the analysts on reviewing the most pertinent information, providing their feedback on the accuracy of those sources and making the ultimate decision on the customer's risk level.

Regarding your enhanced due-diligence process – i.e. additional validation of a potentially risky individual either during initial or periodic review – what is the average or expected time to complete an investigation?

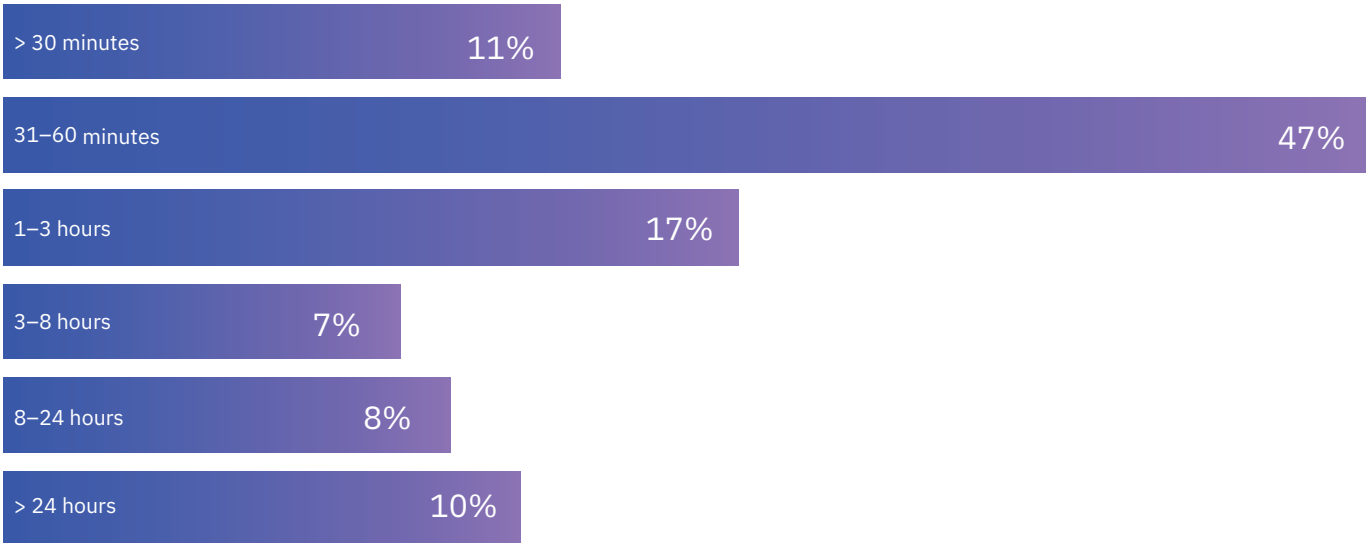

Figure 3: Risk.net Survey Report "Smarter thinking around financial crime prevention", January 2019

Customer case study

Top 20 US bank conducts 60 percent faster EDD investigations

Business challenge

This large, regional financial institution was dealing with a two-fold challenge in its enhanced due diligence (EDD) process. First, its review process was highly manual, lengthy and required too much data entry. Second, due to the subjective nature of these investigations, the results were inconsistent from analyst to analyst and had a high number of errors. In addition, understanding the outcome rationale during the audit process presented a time-consuming and ongoing challenge.

The bank turned to IBM Financial Crimes Insight to help create an EDD process that was more efficient, accurate and standardized.

Transformation

- **Automate data gathering and prioritization:** Instead of requiring analysts to gather data, the solution automatically started gathering information on the entity once the alert was triggered. It aggregated information from structured and unstructured data sources, including sanctions lists, business directories and search engines. The solution then ranked and categorized the data based on its relevance and source.
- **Analyze information using NLP:** Next, Financial Crimes Insight used Natural Language Processing (NLP) to understand the context and sentiment of articles and other information related to the entity being reviewed. This information was then prioritized and annotated for analyst review, helping the analyst understand relevant risk more quickly, as well as why each article was chosen.
- **Simplify investigation and audit reporting:** As a final step, the solution collected the information used to make the customer risk decision into an automated dossier for easier reference during the audit review, which often takes place weeks or months later.

Results

- **Conducted 60 percent faster reviews:** Reduced investigation times from more than 13 minutes to just over five minutes by automating much of the manual search and data entry process
- **Gained a 50 percent reduction in rework:** Minimized the need to retrace investigation steps by automatically collecting comprehensive information in the investigation dossier

Business impact

- **Increased analyst productivity:** By reducing the amount of time for each investigation, analysts can complete more investigations and focus their efforts on analysis instead of data entry.
- **Improved outcome consistency:** Using NLP, the solution can apply the same logic across any written information source, eliminating subjective interpretation due to analyst fatigue or varying interpretation.
- **Reduced audit effort:** With an automatically created dossier, the typical time and effort to understand and recreate the analyst's decision rationale is virtually eliminated.

3. Use case:

AI detects payments fraud faster

Innovation in the payments space is at a level not seen in decades. From mobile payments to peer-to-peer (P2P) payments to real-time payments, there are a growing number of payment services, channels and rails for consumers and businesses alike. But these myriad options also give fraudsters plenty of openings for exploitation, as well.

Easy-to-exploit issues with these new payment services include their speed and lack of transactional and customer behavioral history. These issues put financial institutions and payment processors in a difficult position. If they block a transaction, they could negatively impact a legitimate user, leading the user to either abandon the platform or use a competitor instead. If the transaction is approved and it's fraudulent, it erodes trust in the payment provider and leads to a loss.

Traditional fraud detection systems were designed for a relatively slow-moving fraud environment. Once a new fraud pattern was discovered, a detection rule or model would be created over a matter of weeks or months, tested and then put into production to uncover fraud that fit those known fraud typologies. Obviously, the weakness of this approach is that is takes too long and relies on identifying the fraud pattern first. In the time it takes to identify the fraud pattern, develop the model and put it into use, consumers and the institution could experience considerable fraud losses. In addition, fraudsters, aware of this deficiency, can quickly and continuously change the fraud scheme to evade detection.

To out-pace fraudsters, financial institutions and payment processors need a quicker and more agile approach to payment fraud detection. Instead of relying on predefined models, applications need the ability to quickly adapt to emerging fraud activities and implement rules to stop those fraud types. Not only should organizations be able to adjust their detection models, the models themselves should be inter-operable with any data science, ML, open source and AI technique—using any vendor. In addition, to eliminate fraud traveling from one area or channel to another undetected, aggregating transactional and non-transactional behavior from across various channels providers greater context and spots seemingly innocuous patterns that connect complex fraud schemes.

Customer case study

STET: France's national payments switch stops fraud and saves millions

Business challenge

The National Payment Switch in France, STET, is owned by a consortium of financial institutions and processes more than 30 billion credit and debit card, cross-border, domestic and on-us payments annually. After being among the first countries to introduce the Clearing House Interbank Payments System (CHIPS) and personal identification number (PIN) countrywide, France's fraud rates were minimal for decades. But as criminals became more sophisticated, fraud losses returned and were roughly double the eurozone average for payment cards.

STET turned to IBM Safer Payments to help assess the fraud risk for every authorization request in real time. This score is passed to banks, issuers and acquirers that combine the risk score with customer information to form a final decision on declining fraudulent transactions.

Transformation

- **Build for speed and resiliency:** Given the high volumes, IBM Safer Payments was engineered to process up to 1,200 transactions per second, and can compute a risk score in less than 10 milliseconds. The switching infrastructure is also distributed to operate 24x7 and design for 99.999 percent uptime.
- **Use limited data to gain understanding:** STET doesn't have any customer data or data from other payment channels. It doesn't even know if a debit and a credit card in its portfolio belong to the same cardholder. However, IBM Safer Payments compensates for this issue by being able to look across all transactions, countrywide, as well as creating deep behavioral profiles for millions of cards and merchants. This insight allows it to detect more sophisticated fraud patterns that are often committed by organized crime.
- **Future-ready payments infrastructure:** In addition to helping ensure stability and scalability, IBM Safer Payments was designed to help STET adapt more quickly to new fraud trends, as well as provide fraud coverage to new and emerging payment types like real-time payments.

Results

- **USD 100 million saved annually:** Reduced investigation times from more than 13 minutes to just over five minutes by automating much of the manual search and data entry process
- **A 1:1 false-positive rate:** Enhanced detection accuracy and the need to retrace investigation steps by automatically collecting comprehensive information in the investigation dossier

Business impact

- **Reduced operational costs:** Time saved in identifying emerging threats can greatly reduce the banks' losses and more accurate rules should lessen false positives.
- **Enabled future-ready fraud prevention:** STET expects to glean insights from its transaction data that will help its team continually devise fraud detection rules even more quickly and accurately.
- **Fueled business growth:** This effective fraud prevention solution increases STET's ability to enter new markets and offer services for newer transaction types, including instant payments and Single Euro Payments Area (SEPA) payments, as well as achieve its ultimate goal of reducing payment fraud in France, Belgium and across the EU.

4. Use case:

AI pinpoints conduct risks across complex channels and activities

Institutional trust has been continuously eroding by incidents of financial service employees using the organization or its customers for their own financial gain. But in large, complex financial institutions, spotting this kind of behavior, has been extremely difficult.

One key aspect is the explosion of available communication streams to conduct and coordinate collusive activities. From insider trading to market abuse to customer suitability, it has become difficult for compliance departments to piece together the intent with the activity. As a result, many incidents are found in time-consuming manual reviews well after the misconduct has taken place and the damage is already done.

The key to stopping these activities quickly is not to react, but to predict when they'll happen, and which employees represent a greater risk. Part of this process is already being done today by scanning emails and phone calls for keywords or phrases that are indicative of improper behavior. But many of these lexicons and surveillance activities are well known and avoided by those seeking to evade detection. Instead, the approach should be to look at sentiment rather than a static list of words, and gather trading activity, as well as conversations from all channels, including email, voice and messaging applications. In this way, changes in behavior can help predict if a frustrated employee is engaging in risky behavior and intercede before it happens.

Customer case study

UK bank expands oversight to improve conduct surveillance

Business challenge

This UK-based investment bank was under significant regulatory scrutiny from US and UK regulators for failing to effectively monitor trader voice communications for high-risk behavior. To prevent further penalties, it needed to scale monitoring across the trade floor from its existing manual approach, which was limited to review 20 traders per month from a population of over 8,000.

The bank turned to IBM Financial Crimes Insight, for a real-time solution that could more quickly identify high-risk communications across thousands of traders.

Transformation

- **Don't start from scratch:** Sophisticated pre-built models cut false positives and ranks alerts based on risk.
- **Address issues before they emerge:** Converting voice into accurate speech-to-text files in real time enabled the bank to identify suspicious patterns indicative of conduct risk, market abuse and client suitability.
- **Combine channels for greater insight:** Enriching voice files with additional trade and digital communications data provides greater context and helps detect complex misconduct behaviors across scenarios and asset classes.

Results

- **Greater than 70 percent accuracy:** Improved the speech-to-text word accuracy rate to improve understanding of voice conversations on often noisy trading floors
- **Expanded surveillance fifty-fold:** Enabled the bank to monitor a larger pool of traders by automating analysis far beyond its existing manual process

Business impact

- **Reduces risk with faster investigations:** The Surveillance Insight for Financial Services solution quickly identified evidence and the reasoning behind alerts for quick and accurate resolutions.
- **Achieves more holistic view of risk:** By expanding the scale of surveillance and data analyzed, the bank can detect more sophisticated misconduct.
- **Lessens compliance costs and effort:** With fewer false positives and prioritized alerts based on risk, the bank can achieve greater oversight without overspending on resources.

IBM point of view:

Financial institutions are gaining value from AI

Financial organizations are gaining value by applying AI, ML and RPA. The customer case studies in this white paper show specific ways that financial institutions can use such cognitive solutions to reduce growing risks. These risks are driven by unmanageable complexity and volume, AML, conduct risk, payments, regulatory compliance and emerging technologies.

> "Financial institutions have been improving their ability to identify customers and monitor transactions by experimenting with new technologies that rely on advanced analytical techniques, including artificial intelligence and machine learning."
>
> **Kenneth A. Blanco, Director of FinCEN, at the 2019 SIFMA Anti-Money Laundering & Financial Crimes Conference**[8]

Checklist for where to start the AI journey

Understanding where to focus and apply AI and cognitive solutions can be a daunting task. But as the regulators have stated, the intention should be to augment and assist your existing financial crime management programs rather than replace them. The question is, which strategic objection aligns with the program that needs the most help?

- **Looking for a compliance customer experience win-win?** If the customer experience is being negatively impacted by slow onboarding or due diligence reviews, that may be an area to apply AI. This project can improve compliance and streamline a clunky process.
- **Tired of doing more with less?** As demand can grow faster than budgets, alleviate the stress on AML transaction monitoring and sanctions alert review teams by applying layered analytics and AI to better prioritize risk and reduce false positives.
- **Want to gain a competitive edge?** With new real-time and P2P payments come new risks. Protect emerging payments rails with ML and AI while tying the new technologies into other systems for a more complete, cross-channel view.
- **Need to protect your reputation and customers?** Help ensure that employees are acting in the best interests of the institutional and customers by spotting risky behavior and outright violations across electronic, voice and email communications.

To what extent are you incorporating artificial intelligence (AI)/cognitive learning capabilities in your organization's risk and compliance programs?

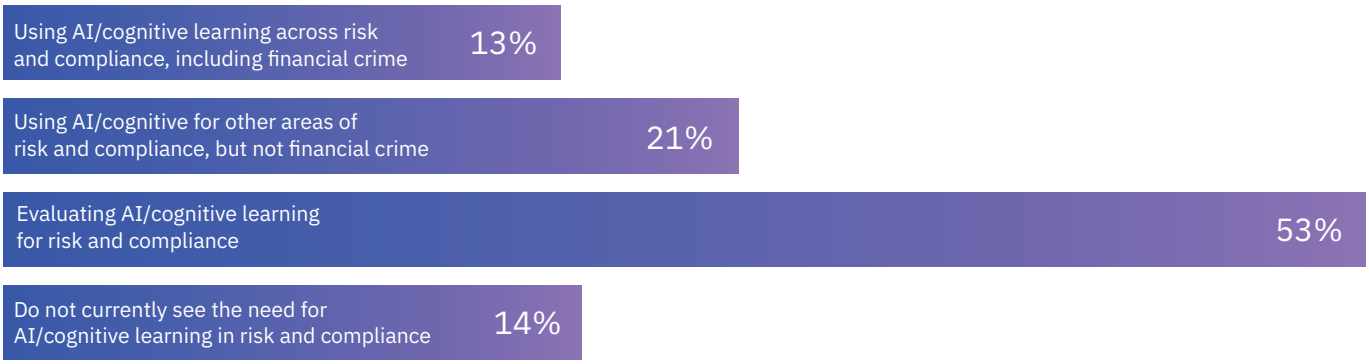

Figure 4: Risk.net Survey Report "Smarter thinking around financial crime prevention", January 2019

Discover solutions that address the challenges facing financial institutions today. For example, IBM Financial Crimes Insight enables financial institutions to leverage IBM Watson® analytics and cognitive capabilities to create an accurate and sustainable AML program. With IBM Safer Payments, banks and payment processors apply AI to enable frictionless payments while maintaining high fraud detection rates.

For conduct risk and insider trading surveillance, IBM Financial Crimes Insight brings a holistic and cognitive approach to monitoring essentially all employee-related activities with increased efficiency and accuracy, and improved regulatory compliance capabilities. It goes beyond traditional rules-based alert detection to pro-actively monitor employees in real time, including emails, chat transcripts, voice recordings, trade and market data.

Next steps:

Why act on AI now?

Financial crime and corruption are at epidemic levels and many countries are unable to significantly reduce corruption.[9] Regulators and financial institutions are looking to innovative AI technology to fix problems that have grown beyond their ability to solve with intuition and existing tools alone. To justify cognitive initiatives, financial services organizations need to show real return on value in such investments. IBM is able to demonstrate the value in a variety of use cases, as shown in the client success stories outlined in this white paper.

A misunderstanding about AI is the belief that it will replace employees. However, the financial crime analyst is and should always be an essential part of this process. AI, process automation and advanced analytics are tools that can perform analyses and tasks in a fraction of the time it would take an employee.

Yet, the ultimate decision-making power still lies with those analysts, investigators and compliance officers for whom this technology provides greater insight and eliminates tedious task work. This augmented intelligence is the next phase of the fight against financial crime, and one that only together financial institutions, regulators and technology partners can win.

About IBM Financial Crimes Insight

By resolving relationships and scrutinizing behaviors to identify high-risk entities before they commit financial crimes, IBM Financial Crimes Insight empowers institutions to increase both the efficiency and the effectiveness of their payment fraud detection, anti-money laundering compliance, know-your-customer, conduct surveillance, and insurance claims investigation programs. Only IBM uses the broadest set of market-leading AI, cognitive services, big data and automation technologies, driven by input from leading regulatory experts to minimize the financial and regulatory burden of compliance while reducing reputational risk.

To learn more about IBM financial crime management solutions for anti-money laundering, fraud prevention, conduct surveillance and insurance claims fraud investigation, visit ibm.com/RegTech and follow us on Twitter @IBMFintech.

Footnotes

1. “Civil Penalties and Enforcement Information.” U.S. Department of the Treasury Office of Foreign Assets Control (OFAC), April 2019. https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx

2. “U.S., EU fines on banks’ misconduct to top $400 billion by 2020: report.” Reuters.com, September 2017. https://www.reuters.com/article/us-banks-regulator-fines/u-s-eu-fines-on-banks-misconduct-to-top-400-billion-by-2020-report-idUSKCN1C210B?il=0

3. “The Troika Laundromat.” OCCPR.com, March 2019. https://www.occrp.org/en/troikalaundromat/

4. “EU sanctions: A key foreign and security policy instrument.” European Parliament Briefing, May 2018. https://www.europarl.europa.eu/RegData/etudes/BRIE/2018/621870/EPRS_BRI(2018)621870_EN.pdf

5. “Specially Designated Nationals and Blocked Persons List.” U.S. Department of the Treasury Office of Foreign Assets Control, May 23, 2019. https://www.treasury.gov/ofac/downloads/sdnlist.pdf

6“Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing.” Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Financial Crimes Enforcement Network, National Credit Union Administration, and Office of the Comptroller of the Currency, December 3, 2018. https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf

7.“FCA Innovate.” Financial Conduct Authority. https://www.fca.org.uk/firms/fca-innovate

8. “Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the SIFMA Anti-Money Laundering & Financial Crimes Conference.” U.S. Treasury Financial Crimes Enforcement Network, February 4, 2019. https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-sifma-anti-money-laundering

9. “Corruption Perceptions Index 2018.” Transparency International.org. https://www.transparency.org/cpi2018 http://content.healthaffairs.org/content/34/3/371.short.

10. Risk.net Survey Report “Smarter thinking around financial crime prevention”, January 2019 https://www.ibm.com/downloads/cas/5QGBKWDB

Doc ID: 82026682USEN-00

Fighting financial crime with AI

Whitepaper

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
December 2019

IBM