WHITE PAPER

# AUTOMATION: Breaking new ground in AML compliance

APRIL 2021

INSIGHT | INTELLIGENCE | INNOVATION

fiserv.

THEMIS

## Introduction

Following the regulatory wave set in motion by the global financial crisis and associated financial crime scandals, regulators have imposed increasingly stringent rules on financial institutions, requiring them to improve oversight by reinventing their compliance processes, including through automation. On 3 September 2020, the Bank of England's (BoE) Governor, Andrew Bailey, delivered a speech focused on recent innovations in payments and the challenges these bring. During his discourse, he highlighted the benefits of innovation to regulators, financial institutions and the public alike:

> "Innovation is a good thing. As authorities and regulators it is not in our interest – the broad public interest – to stop innovation. Moreover, when supported by clear standards and expectations, innovation can support the pursuit of public interest objectives such as greater inclusivity and network resilience."[1]

At the same time, the cost of Anti-Money Laundering (AML) compliance is growing along with the need. In April 2020, the Europe, Middle East and Africa (EMEA) region was reported to be spending USD 137 billion on financial crime compliance annually.[2] It is clear that both financial institutions and regulators need to find more effective solutions to tackling financial crime. Given its ability to perform routine compliance tasks faster and more accurately than human resources, automation may represent a good answer.

Automated AML solutions can be placed on an 'intelligence' continuum, with robotic process automation (RPA) representing the simplest component on this continuum, and the next step up being more intelligent forms of automation that integrate robotics with other emerging technologies. Artificial intelligence can be found furthest along the spectrum.

RPA is defined by IBM as a solution that "mimics the actions of human users to perform repetitive and high-volume tasks, freeing people to focus on higher-value tasks."[3] The robotics market is currently in great expansion, experiencing annual growth of 60 percent and bringing in revenues that, according to Gartner, are set to reach nearly USD 2 billion in 2021.[4] This success is thanks mainly to the enthusiasm of financial institutions, which are looking for ways to leverage robotics to meet their compliance requirements in a more accurate and cost-effective way.[5] Indeed, most global banks are investing heavily in RPA technologies and conducting proofs of concept (PoCs), including in order to potentially move from basic to more intelligent forms of automation, as

---

[1] Bank of England, "Reinventing the Wheel (with more automation)" 03 September 2020, https://www.bankofengland.co.uk/-/media/boe/files/speech/2020/reinventing-the-wheel-with-more-automation-speech-by-andrew-bailey.pdf?la=en&hash=6B5DE50DC09345C4D88FA9BF6CC1F660CA742FD4/ (Accessed: 15/01/2021).

[2] Nicodemus, A. "Study: Europe blows U.S. away in financial crime spending" Compliance Week 07 April 2020 https://www.complianceweek.com/aml/study-europe-blows-us-away-in-financial-crime-spending/28718.article (Accessed: 15/02/2021).

[3] IBM, "Fighting financial crime with AI" https://www.ibm.com/downloads/cas/WKLQKD3W (Accessed: 15/01/2021).

[4] Gartner, "Gartner Says Worldwide Robotic Process Automation Software Revenue to Reach Nearly $2 Billion in 2021" 21 September 2020, https://www.gartner.com/en/newsroom/press-releases/2020-09-21-gartner-says-worldwide-robotic-process-automation-software-revenue-to-reach-nearly-2-billion-in-2021#:~:text=RPA%20Market%20Forecast%20to%20Grow,latest%20forecast%20from%20Gartner%2C%20Inc (Accessed: 15/01/2021).

[5] Transparency Market Research, "Robotic Process Automation (RPA) Market" https://www.transparencymarketresearch.com/robotic-process-automation-market.html (Accessed: 15/01/2021).

described above. A combination of robotics with more intelligent and autonomous systems can bring powerful transformation to AML compliance.

This paper seeks to examine the role of automation in AML compliance, outlining a few key use cases and assessing current regulatory approaches. The analysis draws upon desktop research and relevant survey findings, highlighting both the benefits and challenges of the adoption of robotics and intelligent automation (IA) in the risk and compliance space.

## Robotic processes and intelligent automation in AML compliance

Governed by business logic and structured inputs, robotic process automation is a type of technology that helps organisations to partially or fully automate standardised tasks. It involves software robots which mimic human action to perform a variety of processes, from data entry and transaction processing to response triggering and communication with other digital systems.

Thanks to its potential ability to increase efficiency in data generation and interpretation, RPA technology is gaining considerable traction in the regulatory compliance departments of financial institutions. According to a report by the Hong Kong Monetary Authority[6] (HKMA), RPA has been one of the most common technologies implemented by banks in Hong Kong for AML/CFT purposes, with roughly 65 percent of those surveyed by the HKMA in 2019 having adopted it. If properly implemented, RPA-driven processes can replicate the majority of tasks involved in AML compliance: RPA mimics human action by capturing data, running applications, triggering responses, and communicating with other systems. Flexible and easy to implement, the software follows the logic of compliance parameters set in place when analysing and interpreting data presented to it. Furthermore, RPA enables internal control of compliance processes, as bots' actions are saved in log files that can be reviewed any time.

Seeing the potential gains associated with automation, many banks are also looking to augment their RPA capability by combining robotics with other emerging forms of intelligent technology, such as machine learning. For example, the Hong Kong Monetary Authority found that two out of five banks surveyed had implemented RPA as a stepping stone whilst considering other more mature technology solutions. The result, referred to as intelligent automation (IA), gives an additional accuracy and efficiency boost to compliance processes, further simplifying interactions and increasing speed. For instance, it has been shown to deliver a significant reduction in false positives and a decrease in the volume of suspicious transaction alerts.

## Use cases

The Fiserv Financial Crime Survey 2020, which surveyed compliance professionals from across the EMEA region about emerging financial crime trends, asked respondents where artificial intelligence and robotics sit in their list of priorities during COVID-19. Despite lockdown circumstances, 46 percent said these technologies were "central to their strategy", with a further 28 percent highlighting AI/robotics as a key area of focus but noting slight de-prioritisation as a result of the pandemic.

[6] Hong Kong Monetary Authority, "AML/CFT Regtech: Case Studies and Insights" January 2021 https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf (Accessed: 01/02/2021).

There are several processes within AML compliance which are particularly suited to robotic and other forms of automation. These include:

- **Suspicious activity alert investigation**: transaction monitoring is the perfect candidate for RPA solution implementation, given that it involves standardised and repetitive tasks related to the management of a large number of alerts. It is also a compliance process that allows for significant coordination between analysts' work and automated solutions: as RPA cannot completely replace analyst knowledge, its purpose is to reduce the workload of human employees by lowering the number of false positives and helping increase the focus placed on highest risk alerts by providing, for instance, risk scores.
- **Customer onboarding**: automated solutions can be implemented as part of Know Your Customer (KYC) document gathering and validation processes, which the majority of respondents to the aforementioned Fiserv Financial Crime Survey 2020 found were the areas of financial crime detection that had been best addressed by technology solutions. The automation of customer onboarding can take different forms, from automated document capture to automated identity verification. RPA/IA can substitute human input in collating data from disparate internal systems or from external sources such as regulatory agencies and open databases, including company registers to identify beneficial owners.
- **Client screening**: firms are also using RPA/IA in Open Source Intelligence (OSINT) research. In this application, robots automatically navigate and collect live data from any website, in multiple languages, in the present moment as well as into the future as sources change. Additionally, RPA can find content hidden within the deep web and navigate complex menu structures, using different crawl techniques to access the volume of sites needed early during investigative work and then pinpoint the depth and precision required as this work proceeds.

### Why should financial institutions invest in IA/RPA solutions?

Businesses, irrespective of size, location or revenue, must ensure that their employees, customers and operations are protected against financial crime. EY estimates that the annual cost of money laundering and associated crimes is USD 1.4 trillion to USD 3.5 trillion[7]. These figures are only expected to grow, with PwC reporting in March 2020 that economic crime had reached its highest level ever over the previous 24 months, with 56 percent of UK businesses surveyed stating that they were impacted by fraud, corruption or other forms of economic crime[8]. In Europe, Europol's European Financial and Economic Crime Centre (EFECC) reported that economic crime costs the EU economy some EUR 110 billion a year, with only a tiny fraction of it, approximately EUR 1.2 billion, subsequently confiscated by authorities[9].

Money laundering and related financial crimes have a serious impact on the global economy and have the capacity to disrupt business operations and damage company reputation. Firms must comply with AML regulations, which continue to tighten as regulators deepen their scrutiny. AML

[7] EY, "Disrupting Financial Crime" https://www.ey.com/en_uk/disrupting-financial-crime#:~:text=Financial%20crime%20is%20an%20enormous,trillion%20to%20US%243.5%20trillion (Accessed: 20/01/2021)
[8]PwC, "PwC's Global Economic Crime Survey 2020: UK findings" https://www.pwc.co.uk/services/forensic-services/insights/global-economic-crime-survey-2020.html#:~:text=Economic%20crime%20has%20reached%20its,the%20global%20finding%20of%2047%25 (Accessed: 20/01/2021).
[9] Banks, M. "European Financial and Economic Crime Centre to take on organised crime" The Parliament, 08 June 2020https://www.theparliamentmagazine.eu/news/article/european-financial-and-economic-crime-centre-to-take-on-organised-crime (Accessed: 15/02/2021).

departments therefore have a critical role to play in protecting their businesses from unnecessary risk and reputational damage and need to find new ways to improve their organisations' ability to handle larger volumes of data with accuracy and speed. The efficiency and optimisation gains, as well as cost savings, associated with robotics can help here.

RPA and IA solutions can increase efficiency as they reduce the need for repetitive, deterministic and manual tasks. According to a Genpact[10] white paper, over 70 percent of enterprise processes can be automated using software robots. Another global study conducted by OnePoll[11] highlighted that the average employee spends more than three hours a day on manual, repetitive computer tasks that are not part of his/her primary job and are susceptible to human error.

This is particularly true for compliance monitoring and screening, which involve especially large quantities of unstructured data. According to the Hong Kong Monetary Authority, the popularity of intelligent automated processes among financial institutions is due to these representing relatively non-invasive solutions with benefits - notably cost takeout and resilience - which are attractive and easy to understand. For instance, RPA can collect and aggregate data from multiple sources faster and more efficiently than employees can. This not only increases the effectiveness of regulatory and risk reporting, but also allows employees to redirect their expertise towards higher value reporting, judgement-based monitoring and investigative analysis.

Another benefit of automation is that it can help businesses reduce the ever-rising cost of compliance by significantly cutting manual data entry. At the same time, it helps firms avoid fines or legal issues by supporting compliance teams in meeting the latest regulatory requirements.

Intelligent automation enables better enforcement of regulation due to the level of process accuracy it offers. Not only do bots eliminate human error in data entry, they can also centralise reporting data into any format required. As a result, they increase institutions' auditability. Since financial institutions are routinely evaluated by regulatory agencies, compliance teams spend considerable time and resources in preparation for a regulator's knock on the door. For instance, RPA can help by providing a near-flawless recording of the processes that are executed as well as their modalities.

### Challenges associated with using intelligent automated solutions in AML compliance

Although the business case for RPA/IA application in the risk and compliance sector is solid, its implementation does not come without challenges. Financial institutions are well aware of the possible complications and some are still somewhat cautious about implementing large-scale intelligent automation.

Many banks lack the frameworks and standards that would help them identify the right processes for these types of automation. In addition, insufficient documentation of existing standardised, manual processes can compromise the effective implementation of new technologies. Financial institutions also often fail to contemplate RPA as a long-term solution, and instead see it as a short term, tactical fix to problems that cannot be addressed through reliance of third parties.

---

[10] Genpact, "From robotic process automation to intelligent automation" https://www.genpact.com/downloadable-content/insight/the-evolution-from-robotic-process-automation-to-intelligent-automation.pdf (Accessed: 20/01/2021).

[11] APNews, "Global Research Reveals World's 'Most Hated' Office Tasks" 21 January 2020 https://apnews.com/press-release/pr-prnewswire/fce1a94aa141a06c8c4235dc0e45cf2c (Accessed: 20/01/2021).

Furthermore, integrating these automated systems often proves more complex and time consuming than organisations initially expect. For businesses adopting these technologies, the first obstacle is the lack of understanding amongst senior management of how automated systems work and what their consequences are. Without a cultural shift in favour of automation amongst senior management, implementation of intelligent automated solutions poses difficulties. This can be prevented with appropriate prior research. However, it is also compounded by regulatory ambiguity over the use of intelligent automation.

The introduction of technology is also transforming employee roles and business processes, posing new challenges related to human-robot collaboration. Without appropriate employee training, the implementation of these solutions may result in confusion, reluctance on the part of employees to adopt automated measures, and concerns about potential job losses. In reality, automated compliance management solutions still require considerable human attention and scrutiny, especially to detect and solve potential technical issues. If employees are not properly trained, any problems that arise may result in delays and service interruption.

When it comes to fears of potential job losses, RPA is unlikely to fully replace underlying business systems. Instead, automation allows companies to redirect employees' attention towards higher value, more analytical tasks. However, lack of understanding of these benefits of technology may cause unwanted friction.

### What is the position of regulators?

Regulators are increasingly showing measured but encouraging approval for automated solutions, recognising the potential improvements that recent innovation can bring to compliance processes. Regulators are using RPA themselves to maximise and increase their monitoring efforts: from a regulatory perspective, any innovative solution that helps analyse the increasing number of suspicious transactions and ensure compliance is welcome. Still, regulatory bodies remain very conscious of the challenges that large-scale implementation of technological tools in compliance may pose.

The Bank of England is not the only organisation to highlight the importance of promoting innovation in the financial sector. The UK's Financial Conduct Authority (FCA) also noted the importance of automation in a 2019 speech by its Executive Director of Strategy and Competition, Christopher Woolard, entitled "The Future of Regulation"[12]. Mr Woolard recognised that innovation had gathered pace in the regulatory sphere, underlined that automation had the capacity to bridge the gap between customers and providers, and said that it was, therefore, of utmost importance for regulators to adapt to the times, including by digitising many of their analogue processes.

A similar approach towards new technologies has been taken by the Financial Action Task Force (FATF), which listed "digital transformation of AML/CFT" as a key objective of the organisation's German Presidency in the 2020-2022 period.[13]

[12] FCA, "Regulation in a changing world" 21 October 2019 https://www.fca.org.uk/news/speeches/regulation-changing-world (Accessed: 21/10/2021).
[13] Financial Action Task Force, "Priorities for the Financial Action Task Force under the German Presidency", http://www.fatf-gafi.org/media/fatf/documents/German-Presidency-Priorities.pdf (Accessed: 01/01/2021).

The FATF had previously analysed the potential use of centralised databases as a means of verifying customers' identities, as well as the potential for artificial intelligence and machine learning to deliver more effective monitoring and screening systems for suspicious financial activity. Finally, the organisation has highlighted the ways in which technology can improve financial access and reduce reliance on cash payments through more efficient processes and lower costs.[14]

In Asia, the Hong Kong Monetary Authority analysed case studies of the use of Regtech in finance, assessing benefits and challenges presented by automation, with a particular focus on RPA. After careful consideration, it concluded that "there are significant opportunities for banks to further adopt established solutions in AML/CFT, and to explore new solutions as they emerge"[15]. As a result, the regulator included Regtech as a key area of focus in its 2021 AML/CFT supervisory programme.

In the United States, the Financial Crimes Enforcement Network (FinCEN) and four other government agencies issued a "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing"[16] in December 2018, in which they encouraged banks to implement innovative approaches and new technology in financial crime prevention.

## Conclusions

Intelligent automated solutions have the potential to improve the effectiveness and efficiency of compliance processes in a number of ways. Firstly, by reducing the need for human work on manual and repetitive tasks, RPA/IA allows businesses to redirect their resources towards more insightful and investigative analysis. Secondly, since they can process high volumes of data in a timely fashion, bots ensure a more thorough monitoring of suspicious activity in an increasingly stringent regulatory environment. Finally, the scalability and flexibility of RPA makes it highly adaptable to the dynamics of different business environments, allowing institutions to be ready for regulatory audit with lesser effort required from their employees.

However, as further opportunities for the implementation of technology in AML compliance arise, such as cognitive or intelligent automation, it is important to keep a few considerations in mind when exploring the rollout of new solutions.

Firstly, RPA/IA enhances process efficiency only if accompanied by thorough staff training, a pro-automation culture amongst senior management and a company-wide understanding of some of the challenges it can present, both in terms of implementation and maintenance. Financial institutions must establish RPA/IA governance frameworks and standards, and continuously update their knowledge of technology tools so as to be ready to integrate ever more cutting-edge forms of automation into their existing processes.

---

[14] Financial Action Task Force, "Dialogue on FinTech and RegTech: Opportunities and challenges" March 2017, https://www.fatf-gafi.org/publications/fatfgeneral/documents/fintech-regtech-mar-2016.html (Accessed: 21/10/2021).

[15] HKMA, "RegTech", January 2021.

[16] 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 "Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing" 3 December 2018 https://www.fincen.gov/sites/default/files/2018-12/Joint%20Statement%20on%20Innovation%20Statement%20%28Final%2011-30-18%29_508.pdf (Accessed: 04/01/2021).

Secondly, more intelligent forms of automation do not come without a cost: financial institutions will need to perform a cost-benefit analysis to understand whether their implementation, which requires training and continuous maintenance, makes sense.

Finally, it is crucial for regulators to provide clearer guidance on the implementation of technology tools and their implications for compliance. If these considerations are kept in mind, the use of RPA/IA in the financial services industry will drive cost efficiencies and reduce manual effort, thus creating exponential value for the end customer, enabling staff to focus on higher value tasks and ultimately ensuring more effective tackling of financial crime.

## Authors


**Maria Nizzero**
Associate Director of Analysis
Think Tank
Themis
Maria.Nizzero@Themisservices.co.uk

**Peter Banham**
Group Manager
Financial Risk Management Solutions – EMEA
Fiserv
Peter.Banham@fiserv.com