AML CHALLENGES FOR FINTECHS: INSIGHTS FOR THE FUTURE

FINTRAIL

REFINITIV®

An LSEG Business

TABLE OF **CONTENTS**

INTRODUCTION

This insights-led paper is designed to serve the anti-money laundering (AML) teams of forward-looking financial technology (fintech) firms that seek to prepare their organisations for 2023 and beyond. Based on exclusive interviews with experts in different fintech industries and geographical markets, this paper provides practical insights and advice for navigating the current and emerging challenges in the AML space.

The last few years have been nothing short of unprecedented. From a global pandemic that dramatically altered customer banking behaviours and internal compliance procedures to colossal sanction regimes against Russia, fintechs and their AML compliance teams have been in the throes of change.

Being agile and adaptable is a core part of the fintech DNA. As industry expected to grow by US$305.7 billion by 2023, fintechs innovative product offerings will continue a growth trajectory as consumer preferences evolve. The fintech industry is motivated to explore opportunities and mature faster than traditional banks, adapting their control environment quickly to deal with dramatic customer base increases, new products, services or markets. As the economic downturn looms with rising interest rates and the slowdown of capital injections, fintechs will be assessing how to maintain a route to profitability, coupled with operational efficiencies and the growing demand for a frictionless, engaging customer experience.

CURRENT **AML** CHALLENGES

Financial crime threats are constantly shifting and evolving as technology advances. Criminals seeking to evade controls are resourceful, quickly making use of new opportunities to conduct illicit activity. Despite varying financial product types and niches, all financial institutions, including fintechs, face common challenges.

ONLINE FRAUD

Fraud is a growing global problem, with some calling the current era a fraud epidemic. In the United Kingdom, where fraud is the most commonly experienced crime[1], reported losses totalled £2.35 billion in 2021[2]. In the United States, fraud eclipses all other proceed-generating crimes[3] and 2.8 million consumers made fraud reports in 2021[4]. Encouraged by opportunities created during the pandemic, where consumer habits shifted, while remote onboarding and digital banking adoption increased rapidly and at the same time, criminals have been adapting their processes to exploit vulnerabilities in financial institutions and bypass their controls.

Unsurprisingly, one of the biggest threats facing all the fintechs we interviewed was fraud. Fintechs cite application fraud through impersonation or use of synthetic identities as persistent threats to tackle, including a rise in increasingly convincing fraudulent and counterfeit documents, which are difficult to detect. Fraudsters are using technology to provide better-quality originals which manipulate information and hide changes by using graphics processing and deep-fake technology. Since fraud is a costly responsibility to bear, encompassing both the value of a fraudulent transaction and the associated compliance resource burden, fraud's enormous impact on a firm's bottom line makes it a top priority.

While fraud remains the current primary concern for fintechs, the consensus view among those we interviewed is that fraud will likely continue to remain concerning for the foreseeable future. One AML department head at a Brazilian digital bank, commenting on the national economic crisis fuelling the conditions for impersonation fraud and money muling[5], states: "It has become much easier for fraudsters to convince people to become a money mule." Interviewees also highlight the vulnerability of customers who may be susceptible to fake investment scams. A head of compliance in a crypto firm says: **"Both in crypto and in the banking space, scam activity is probably the highest that I've ever seen."**

Bad actors are active in both the crypto and fiat worlds, often with social media enticing people with 'get-rich, quick' scams. Fintech firms tell us that they are focused on education and raising awareness to help keep customers safe. They also explain that they are increasingly engaged with government bodies. This engagement includes Singapore Police Force's Anti-Scam Command (ASCom) Centre, which launched in March 2022 and works with financial services and crypto firms to share intelligence through communication to quickly freeze accounts, reduce losses and recoup funds for those impacted[6]. AsCom has since opening helped seize US$10 million, which is the largest amount recovered from a single case to date. Other initiatives include the relaunch of the UK's Joint Fraud Taskforce[7] and the creation of the US Secret Service's Cyber Fraud Task Unit[8]. These organisations bring together the private sector, governments and law enforcement agencies to deter and disrupt fraud and cybercrime through sharing intelligence, best practices and resources.

0.2

" Fraud is not a cost of doing business that can be ignored, it needs to be actively managed."

ANTHONY JERKOVIC,
Director of Data,
Novo

[1] National Audit Office, 2017
[2] Action Fraud, 2020-2021
[3] National Money Laundering Risk Assessment, 2022
[4] Federal Trade Commission, 2022
[5] Money Mule
[6] Singapore Police Force
[7] Joint Fraud Taskforce
[8] Secret Service

DIGITAL ASSETS AND CRYPTOCURRENCY ADOPTION

From a consumer perspective, global crypto adoption is steadily rising, higher than pre-bull market levels[9]. Coinciding with this rise in popularity, cryptocurrency regulation has made monumental recent advancements including the European Union's landmark Markets in Crypto Assets (MiCA), which seeks to bring clarity to the so-called 'wild, wild west' of cryptocurrency. While MiCA addresses the crypto Travel Rule in the EU, a targeted update by the global money laundering and terrorist-financing watchdog, the Financial Action Task Force (FATF) noted an overall slow implementation, with only 29 out of 98 responding jurisdictions having passed Travel Rule legislation as of March 2022[10]. Globally, cryptocurrency-related legislation is advancing and the requirements on virtual asset service providers (VASPs) operating across many jurisdictions will increase. These combined factors stress the growing need for all fintechs to consider the risks and exposure associated with the more widespread adoption of digital assets.

Digital assets fintechs must create and review their risk-rating methodology to consider the nuances of different cryptocurrencies and non-fungible tokens (NFTs). While some digital assets may be perfectly legitimate and held for long-term investments, others may be a pump-and-dump scheme like the 'Squid Game' coin or a Ponzi scheme like 'One Coin'. Another challenge in the virtual-asset space is the quick pace of change with product and technology development. Risks from decentralised finance (De-Fi) technologies, exemplified by the recently sanctioned virtual currency mixer Tornado Cash that was used to launder more than US$7 billion since 2019[11], must be considered. It is inherently challenging staying on top of new asset classes, their functionalities and potential risks. Firms must continually learn to understand associated risks and leverage as much data and automation to understand what kind of typologies need increased focus. To manage this, it requires "being nimble in terms of rule sets and investigation priorities", says Tarik Erk, the Head of Regulatory Compliance Asia at Crypto.com.

Fintechs we interviewed underscore the importance of deciding which product falls within a firm's risk appetite for buying or selling. For fintechs that don't bank digital assets, assessing how they interact with VASPs is also critical. For example, considering whether inbound or outbound fiat transactions to and from exchanges are allowed, and if so, which VASPs are considered within the risk appetite. Bridging the understanding gap internally as firms open up to digital assets will be crucial in managing risk appetite.

The Global Coalition to Fight Financial Crime

A public-private partnership coalition, has created the Digital Asset Task Force, bringing together industry leaders committed to effectively fighting financial crime. While the industry is broad and diverse, all members of the Digital Asset Task Force share the same fundamental beliefs, which are also the core objectives of the Global Coalition to Fight Financial Crime. These include the need to increase collaboration, share information and leverage innovation and technology, all to generate a more effective response.

[9] Chainalysis, 22022 Global Cryptocurrency Adoption Index - Chainalysis022
[10] FATF, June 2022
[11] OFAC, 2022

SANCTIONS

One of the biggest challenges for AML teams in 2022 is keeping on top of the tremendous number of Russia-related sanctions in response to the war in Ukraine. In this context an unprecedented number of sanctions packages have been issued, including the most comprehensive and severe sanctions ever imposed on a major economy. Teams have been extremely challenged to remain compliant with the pace of enormous and far-reaching sanction regimes, highlighting the truly dynamic spirit of AML compliance. Though they garnered the most headlines, sanction changes are not solely focused on Russia.

Another example is the United States' Executive Order 13959, which had consequences for buy-side firms concerning Chinese military companies' sanctions[12] and fresh sanctions on Iran in response to state violence. The consequences of sanctions violation can be steep, as highlighted by a recent action brought by the U.S Treasury Department of Treasury where Bittrex, a cryptocurrency exchange, agreed to pay a US$29 million fine for failing to prevent individuals from sanctioned jurisdictions such as Crimea, Cuba, Iran, Sudan and Syria from using its platform[13]. These cases underscore the inherent link all financial institutions have to global politics and its consequent fragile and ever-changing landscape.

Fintechs contended with Russian asset flight risks and enormous spikes in alerts that forced internal resource shifts to meet demands. Some fintechs were fined for breaching sanctions, including a UK payment processor that was cited as having a poor understanding of financial sanctions[14]. This UK case highlights the difficulties in not only resource allocation but also interpretating and understanding sanctions. The prevailing exposure to sanctions risk is likely to continue in 2023, with one fincrime intelligence director at a large digital bank saying: "I don't see the focus on sanctions risk changing significantly over the next 12 months."

Reinforcing the focus on Russia, the EU has recently adopted its eighth package of sanctions, which includes a full ban on crypto-asset wallets, accounts or custody services to Russian persons and residents[15]. Fintechs and their sanctions teams will need to remain alert and agile to increasingly stringent requirements.

[12] The White House 2021
[13] Reuters 2022
[14] Office of Financial Sanctions Implementation HM Treasury
[15] European Council 2022

INDUSTRY TRENDS

In light of their faster maturity models and the dynamic risk landscape, the industry trends that fintechs face help shape their response to their most pressing financial crime threats.

USE OF TECHNOLOGY AND REGULATORY GUIDANCE

> “ In my experience, the best way to try and have a control environment that’s effective and efficient, but importantly, explainable to regulators, is to have a combination of machine learning models anvd heuristic models.
>
> The heuristic models are helpful in being able to demonstrate that you have a clear view of what financial crime typologies are relevant to your customers, your products or services, and your markets and very importantly, rules which provide coverage for them.”

JESSIE APPLE
Compliance Director, Airwallex

Regulators worldwide are increasingly expecting larger and complex firms to use technology to address money laundering and terrorist financing threats. According to FATF, applying new technologies makes tackling financial crime faster, cheaper and more effective[16]. The Wolfsberg Group also named technology a “key enabler” in effectively identifying financial crime risk on a real-time basis[17]. In our interviews with the fintech community, they say machine learning and artificial intelligence (AI) are indispensable tools for identifying financial crime, especially as their businesses grow and volumes of transactions and customers increase. However, one of the biggest challenges is factoring in explainability, a component that regulators are increasingly scrutinising.

A financial crime director at a large digital bank tells us it is important to explain technology as you go along, rather than waiting to the very end when the reasoning behind small and incremental decisions could be lost. Highlighting this, the interviewee adds: “It’s important to have that very clear narrative for any external person, especially in a manner that isn’t loaded with technical jargon that could be perceived as smoke and mirrors or a black box.” Fintechs also suggest a combination of machine learning models and heuristic models to advance efficiency and explainability.

When discussing implementation with interviewees they suggest assessing the following to ensure AI’s explainability:

- Have you effectively collaborated with your internal stakeholders to identify the needed technology?
- Have you translated capabilities into layman’s terms (without losing meaning?)
- Have you documented your decisions and maintained an audit trail?
- Have you composed a coherent jargon-free standalone document that articulates your evidence and rationale for implementing technology?
- Do you have the correct context?
- Do you have quality, robust and relevant data to support your decisions?

[16] FATF: Opportunities and Challenges of New Technologies for AML/CTF
[17] Wolfsberg Group, Negative News Screening FAQs, 2022

DATA

For AML technology and AI tools to function correctly, having robust and quality data is essential. Data collection must strike a balance between not causing too much friction at the beginning of a customer's journey, which damages the overall experience and could force users off a platform, to too little, which attracts and onboards malicious actors. Striking this balance is foundational for meaningful data analysis and the balance of a firm's profitability and compliance obligations.

Once robust and quality data is obtained and analysed by AI tools, it can produce better and more effective outputs. This meaningful employment of data, which links data with data to tell a story and provide a clear analysis, supports a proactive risk management approach, creating an important component for fintechs looking to optimise efficiency.

GOVERNANCE AND GROWTH

As fintechs scale, an important component of success is effective governance. In a climate where fintechs can experience hyper-growth and a faster maturity curve, keeping up with changing AML controls requires fintechs to shift their focus to adopt a more robust governance model. A compliance department head at a payments service firm says: "Execution and risk management and ownership internally of key risks are still issues, particularly on the product and tech delivery side." To counter this, David Dry, Director of Regional Compliance Asia Pacific, notes: "When you're in a fintech striving for growth, having risk teams and institutional pillars of risk management are important."

Governance needs to evolve with your company. The governance model your company needs now could have been complete overkill five years ago when there was only one product or market to serve. There should be conscious recognition that governance models need to adapt over time as a firm grows.

SCALING AND HIRING FINANCIAL CRIME TEAMS

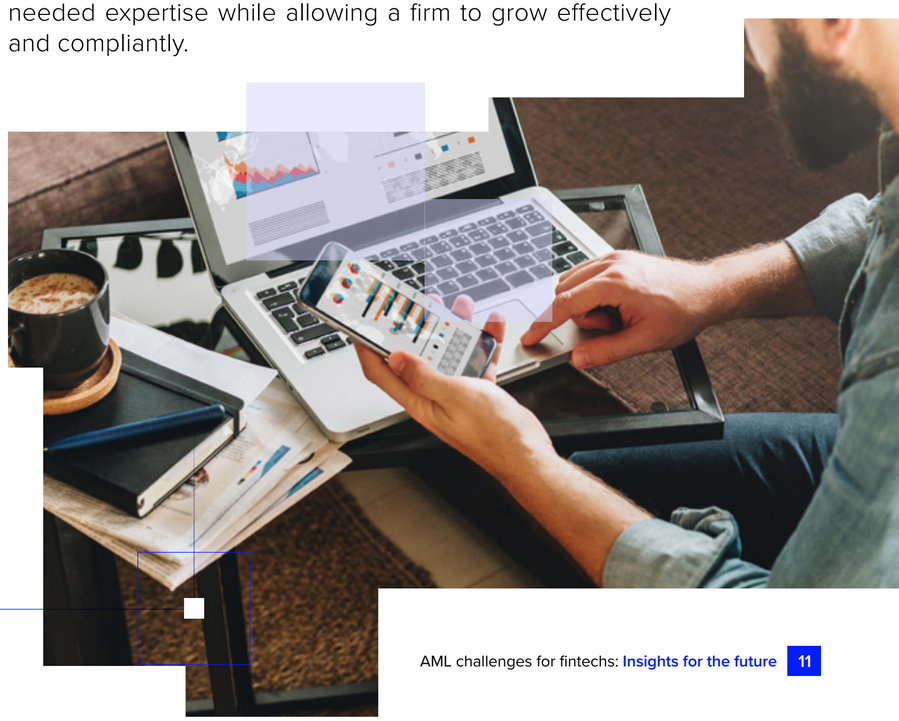
> “ The people that define how controls are implemented (as opposed to those who only define what the requirements are) are a big focus in terms of resource budget allocation because coming up with a very detailed technical proposal for how we’re going to do something is time-intensive and key to ensuring the design and operation of your controls is on point.
> If you think about being lean, I would say in terms of numbers; the biggest focus is resourcing those who define the ‘how’.”

JESSIE APPLE
Compliance Director, Airwallex

While harnessing technology is undeniably important for combating financial crime, teams of people are equally important in supporting the financial crime function. Fintechs tell us that from the first and second line of defence to engineers and data scientists, finding talent to scale is an essential consideration. One interviewee at a large international bank says there is importance of “hiring people who speak each other’s language” and “having that right mix of technical people versus financial crime subject matter technical expertise”. Fintechs also emphasise the continual need to invest in machine learning and data, with engineers and data scientists being key resourcing hires for the years ahead.

Although labour-hiring markets in 2022 swung from the Great Resignation to more uncertainty because of recessionary concerns, financial crime compliance is largely regarded as recession-proof. Given this view, financial crime compliance roles will likely remain in an employee’s market, boasting competitive salaries despite a broader employee pool with remote-working opportunities. Attracting, developing and retaining employees is instrumental to scaling effectively in any market or economy.

Firms experiencing increasing and sudden alert volumes through new sanctions regimes or strong customer growth have also turned to managed services for additional support. Balancing a firm’s growth with increasing regulatory scrutiny means looking at outsourced solutions to practically address short-term demands and process challenges. These solutions can help maximise existing resources and provide much-needed expertise while allowing a firm to grow effectively and compliantly.



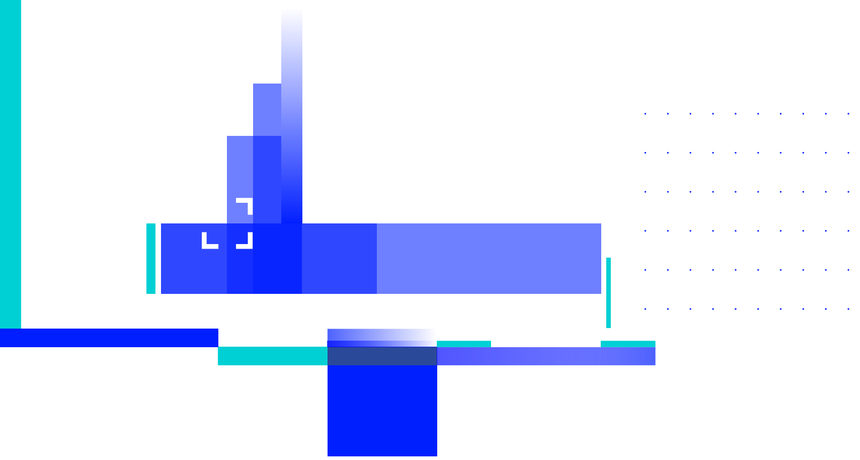
PRIORITISING EFFECTIVENESS AND EFFICIENCY

As technology advances, dynamic risk assessments and scoring models promise greater efficiency. Integrating different internal data points – like geolocation or external data sources such as fraud scores alongside behavioural biometrics – can be used to detect suspicious activity at onboarding, reduce instances of fraud and account takeover, and minimise false positives.

Other data points like device identification can determine if devices are used to access more than one account. Device identification data can also ascertain if an account is being accessed from a new device or number. Comparing this information to the client's history to understand activity is a valuable control in stopping frauds such as SIM swaps or multi-accounting.

Our interviewees stress the importance for fintechs to be dynamic in their risk approaches, focusing on where the real risks exist and not wasting resources. Fintechs say this consideration is especially important in a context where fintechs are naturally lean. However, in tandem with the deployment of new technology, more mature fintechs ¬– focusing on improving output and case management – are increasingly prioritising how effectiveness and efficiency are addressed through other means. By optimising throughput, your process is more efficient. Firms that have been in the market for a few years are now looking for tools that support capacity management from an optimisation standpoint.

As one fintech interviewee highlights: "Five years ago, cases may have been managed end to end by a couple of analysts. Volumes have evolved and we've now had to build out a level-one, level-two and level-three organisational structure within those teams. The priority is the process and the efficiency of the process, rather than increasing the sophistication of the investigation."



"The risk landscape is evolving, but so are the controls. It's a super-exciting space to be in because we're able to move and implement things that are smarter, better, faster."

JESSIE APPLE
Compliance Director, Airwallex

LOOKING FORWARD

Given the current backdrop of financial crime challenges and overarching industry trends that fintechs face, looking ahead to 2023 offers some indication of what they need to prepare for.

REGULATORY CHANGES AND OPPORTUNITIES

Just as financial crime threats evolve, so do regulatory changes and requirements. Following the abundance of crypto regulatory developments in 2022, including MiCa and US President Biden's White House framework for crypto regulation, more regulatory guidance can be expected ahead. Fintechs we interviewed say that jurisdictional differences are also essential, especially in the virtual asset space where regulation is uneven and emerging. Firms must remain agile in response to these upcoming changes and be aware of opportunities. One fintech professional at a global crypto firm stresses the need to have a "global but local" approach, leveraging the resources of a global company and worldwide view, but heeding local operational and regulatory requirements, opportunities and nuances.

Fintechs highlight opportunities for dialogue with the regulators, underscoring the importance of fintechs collaborating with regulators when possible. One example was Singapore's fruitful consultation period with the industry during the introduction of the Payment Services Act, says one interviewee. Another recent example is Dubai's new Virtual

> **"One of my favourite parts of my role is getting to meet with regulators and sharing what we know to be things that help us operate well in a market or things that can be more difficult from a practical standpoint."**

TARIK ERK
Head of Regulatory Compliance Asia
at Crypto.com

Asset Regulatory Authority, which provides ample opportunity for meaningful consultation. Techsprints and regulatory sandboxes, like those by the UK's Financial Conduct Authority[18] and Dubai's Financial Services Authority[19], demonstrate how regulatory technology firms can support the ecosystem, creating innovative solutions for greater anti-financial crime efficiency.

The director of compliance at a payment service business, commenting on the increasing importance and role of fintechs in the regulator's view, tells us: "I think there is an understanding at the regulator level that fintech and non-banking service providers are significant players. Especially when regulators know that they don't fully understand the industry, we as fintechs can speak up and feel like we truly have a voice — like we are heard."

Interviewees note the success of collaboration with the fintech community and that they are observing regulators in regions such as APAC reorganising their teams internally to oversee larger fintech businesses. Another UK fintech discusses setting up a direct dialogue with law enforcement to provide specific analysis backed by data on trends and concerns regarding specific safeguarding concerns raised by their vulnerable customer team to provide intelligence above and beyond the suspicious activity report (SAR) regime.

> **"I'm in this to catch bad people. Feedback is everything because that's the only way I know I'm doing right. I've seen in Australia how that can be extremely effective. I'd like to see that barrier brought down in other places."**

DAVID DRY
Director, Regional Compliance,
Asia Pacific

[18] Financial Conduct Authority
[19] Dubai Financial Services Authority

THE POWER OF THE FINTECH COMMUNITY

The Fintech FinCrime Exchange (FFE) brings together a global network of fintechs to collaborate on best practices in financial crime risk management.

By sharing information on criminal typologies and controls, members help strengthen the sector's ability to detect and counter the global threat of financial crime.

Given fintech's inherently quicker pace and faster maturity curve than traditional banks, AML teams should look for opportunities to leverage one another's experience and expertise to fight crime more effectively. Fintechs that shared their views emphasise the importance of learning from one another to keep up with industry challenges. One interviewee highlights the benefit of sharing information on trends and typologies: "We try to keep our eyes and ears open. Any platform where we can stay connected to a broader community is helpful."

The Wolfsberg Group in a recent paper stressed this power of collaboration, noting how operating in isolation significantly hinders any financial institution's effectiveness. Both Public-Private Partnerships and Private-Private partnerships hold significant value in the fight against money laundering and other financial crimes. Anthony Jerkovic, Director of Data at Novo, a small business financial platform and checking account provider, shares advice for emerging fintech firms: "There is an amazing community within Fincrime. The FFE is a great example of that. Talk with people, work with people and help others. Always remember what you are learning is gold and you need to figure out the way to keep that and build that into products and controls."

EVOLVING CONSUMER DEMANDS AND EXPECTATIONS

Technology informs how people do business and banking, upholding consumer appetites for faster outcomes and instant gratification. In a recent PWC survey, 73% of respondents identified customer experience as crucial in their purchasing decisions and high up on their business priorities. Like millennials, generation Z values instant results and convenience[20], putting pressure on all businesses, including fintechs, to meet these needs.

Among fintechs' struggles is striking a balance between customer service and the right level of friction for AML compliance. Finding ways to reduce friction but maintain compliance requires fintechs to collaborate with different business lines. One interviewee highlights the need to find common middle ground or compromise between product and compliance business lines, noting that much of what is required by regulators is implicit rather than explicit, creating room for discussion and debate. Remaining agile and innovative while balancing compliance requirements is the common goal all are striving towards, and firms are looking to the wider industry solutions to support this. Many fintechs say using digital identities is one solution for a frictionless customer onboarding journey, which have been implemented in some jurisdictions, most notably the Nordics and India.

While it is contingent on jurisdictional availability, the use of digital identities can prove fruitful in tackling fraud and impersonation through the onboarding process. MyInfo in Singapore, a government tech centralised KYC solution, was said to lead to lower fraud or account takeover rates.

> **"Where we can we leverage automation because it's a balance between our compliance needs and customer experience. We want to make sure that customers can get on the platform in a compliant way, and that needs to be as seamless as possible."**

TARIK ERK, Head of Regulatory Compliance Asia at Crypto.com

[20] PWC

TARGETED HELP, AVAILABLE WHEN YOU NEED IT

Refinitiv delivers a comprehensive range of solutions that empower fintechs to tackle AML and KYC related challenges and meet evolving regulatory obligations. More than this, all our solutions have been designed to champion customer centricity and promote seamless, digital experiences. Our solutions are scalable, cost-efficient and designed to help fintechs make better risk-based decisions that maximise opportunities, while protecting against regulatory and reputational damage. Leveraging the combined power of leading technology, trusted data and human expertise, we offer targeted help when and how you need it.

Risk screening solutions

Our World-Check Risk Intelligence database delivers accurate, structured data to help you screen for heightened risk individuals and entities. Offering global coverage across 240 countries and territories, our database can be used to optimise your AML, KYC, sanctions, and anti-bribery and corruption compliance.

The World-Check team monitors all major international and national watch lists and sanctions lists published by governments and independent, non-government bodies and is constantly updated. Access over 5 million active records and pinpoint potential risk early in the game.

Due diligence solutions

Where heightened risk is detected or suspected, our due diligence reports deliver targeted insights to match your exact needs – we offer variable speed of delivery and depth of insight, as required.

Our quality research is delivered by one of the largest in-house analyst teams in the market, staffed by over 500 analysts speaking 65 languages, and supported by a global network of trusted professionals delivering on-the-ground intelligence. The result is complete, consistent due diligence that equips you to manage and mitigate the varied risks within your business relationships.

Identity verification solutions

It is essential that fintechs verify the true identities of customers, but highly sophisticated criminal activity can complicate this process. We deliver low-friction, data-first identity verification for both individuals and entities, helping you to protect the experience of your target customers, while pinpointing illicit activity.

Access our comprehensive, best-of-breed identity verification solutions to identify bad actors, spot synthetic identities, and mitigate fraud within your organisation.

Account verification solutions

Our account verification tools bring together identity verification, account verification and account ownership authentication to deliver real-time solutions that help you minimise payments risk and reduce unauthorised returns.

Access our leading identity verification, bank account verification, and transaction authority authentication tools to tap into account status information for consumer and business accounts and verify that a customer is an authorised signatory prior to processing a payment.

Onboarding solutions

Effective digital onboarding must balance the need to comply with AML and KYC regulations, while protecting the all-important customer experience.

While fintechs are required to conduct thorough checks during onboarding, the combination of scarce resources and large volumes of customers can present a challenge. Our digital onboarding solution solves this challenge by providing cost-effective, highly configurable, zero infrastructure tools that let you seamlessly onboard clients and simultaneously leverage our powerful risk data – from global ID, verification and screening data to document and biometric checks, bank account verification and more.

CONCLUSION

Fintechs have been at the forefront of innovative solutions and a streamlined customer experience, overcoming unique AML challenges and an evolving risk landscape. The challenges of 2022 will largely continue into 2023 as fintechs adjust to developing sanctions, demanding customer expectations, deploying technology to improve operational efficiencies and detect anomalies, while continually managing increasing fraud risks. Successfully meeting these challenges will require maintaining robust data quality to ensure your controls are operating effectively and managing the right governance framework to support decision-making and the regulatory engagement.

At the time of writing this paper in October 2022, an economic recession looms coupled with a European energy crisis, meaning being lean, agile and protecting the bottom line is more important than ever. To overcome future obstacles, fintechs will need to focus on educating consumers on the fraud risks they face. They will also need to upskill their human financial crime teams while employing technology and AI tools that improve profitability and efficiency. Leveraging collaborative opportunities with regulators, governments and other fintechs can produce fruitful results and give a firm a competitive edge.

As 2022 ends, forward-thinking fintechs must ramp up their efforts to protect their viability while championing customer experience and return on investment. To equip your fintech's anti-financial crime compliance team with proven and cutting-edge AML and KYC technology connect with Refinitiv's specialists here.

KEY TAKEAWAYS

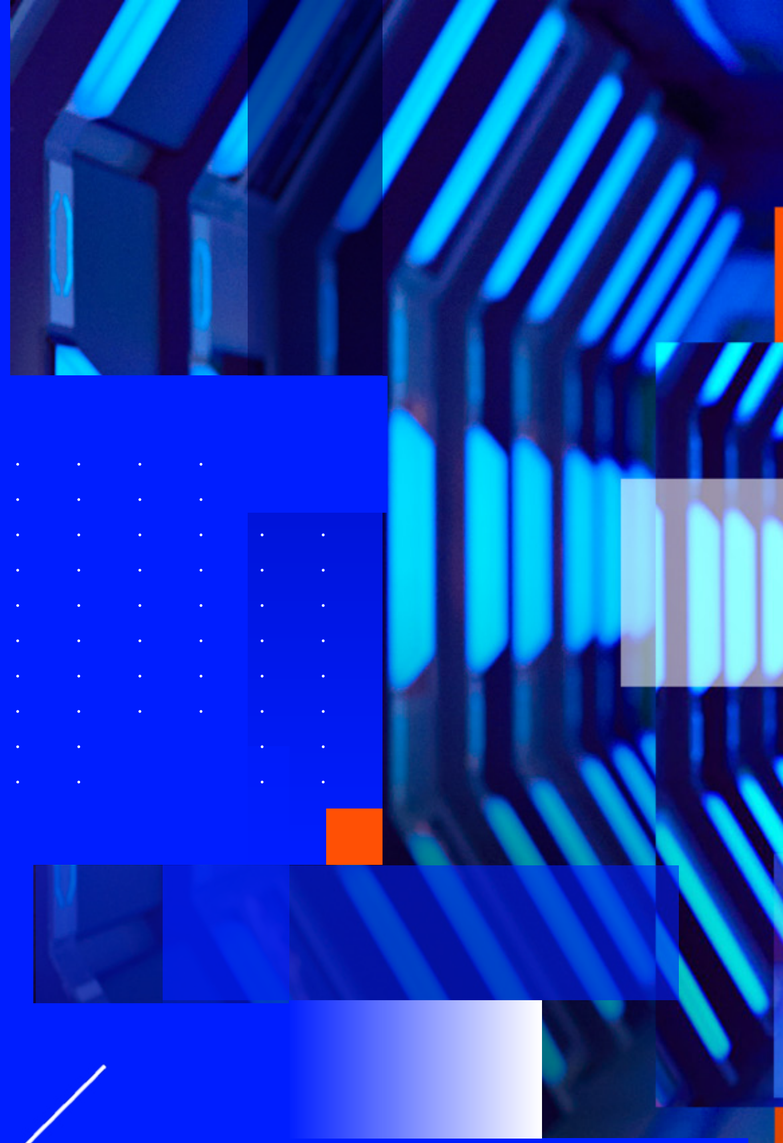
- **Financial crime compliance is recession-proof and firms should focus on upskilling financial crime employees.**
- **Championing customer experience while protecting compliance and profitability will be an important balancing act.**
- **Regulators are increasingly expecting more sophisticated solutions that harness technology capabilities.**
- **Data quality and a robust data set are key to the effective deployment of AI solutions.**
- **Opportunities for community and collaboration with fintechs, government and regulators should be leveraged.**

About **REFINITIV**

Serving more than 40,000 institutions in approximately 190 countries, Refinitiv offers a range of market-leading products, tools and enterprise solutions to support effective regulatory and reputational risk compliance management. Refinitiv provides advanced data and compliance technology and research to help clarify, manage and mitigate risks.

About **FINTRAIL**

We're a global consultancy helping financial services firms manage their exposure to financial crime risk and maintain regulatory compliance. We combine deep financial crime risk management with industry experience to help you prepare for and overcome the challenges of 2023 and beyond.



Visit refinitiv.com | @Refinitiv Refinitiv

Refinitiv, an LSEG (London Stock Exchange Group) business, is one of the world's largest providers of financial markets data and infrastructure. With $6.25 billion in revenue, over 40,000 customers and 400,000 end users across 190 countries, Refinitiv is powering participants across the global financial marketplace. We provide information, insights and technology that enable customers to execute critical investing, trading and risk decisions with confidence. By combining a unique open platform with best-in-class data and expertise, we connect people to choice and opportunity – driving performance, innovation and growth for our customers and partners.

RE2584483

FINTRAIL

REFINITIV®

An LSEG Business