fenergo | Report

Integrated KYC and Scaling for Success

Challenges and Approaches to KYC and AML Transaction Monitoring at Fintechs

In collaboration with FINTRAIL and senior compliance executives at Wise, Banking Circle, and ClearBank

FINTRAIL

Contents

Introduction

Fintechs contend with an ever-changing environment of financial crime typologies, technological innovation, and rigorous compliance regulations.

In 2022, the total enforcement fines for anti-money laundering (AML) related compliance breaches rose globally by 52%[1] (Figure 1), indicating firms are still struggling to meet their compliance obligations. With a rapid industry-wide shift to digital client onboarding, financial crime risks are heightened.

While firms of all sizes face compliance challenges, fintechs must meet them while under pressure to grow and become profitable. How a compliance system - covering both onboarding and ongoing monitoring - matures in line with a fintech's growth is crucial to the firm's survival.

This report combines data from a survey of global fintechs carried out by Fenergo and interviews with financial crime compliance experts at leading global fintechs, in order to glean real-world insights into the sector's top challenges and priorities.

Focusing on two essential anti-financial crime processes, know your customer (KYC) and transaction monitoring, our research demonstrates how vital the integration and optimizing of compliance systems is to scaling successfully.

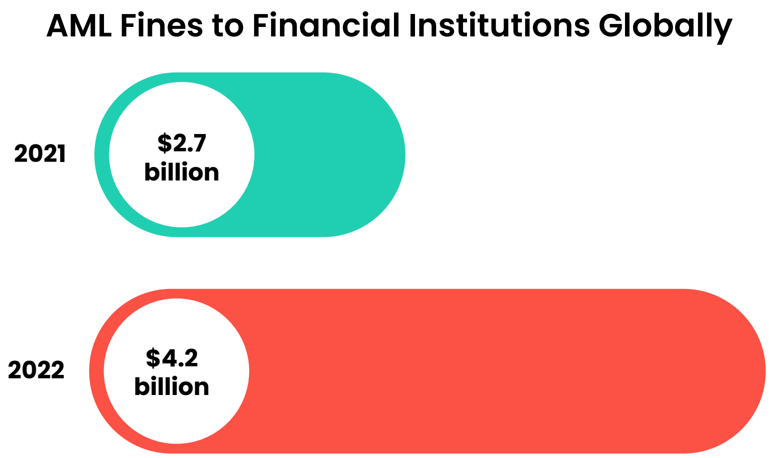

Figure 1

[1] Fenergo

What is KYC?

When a customer initiates a relationship with a financial institution by opening an account, compliance teams must first identify and verify the customer's identity. This goal underpins the KYC process. It involves understanding the expected activities of the customer's account, including identifying and assessing the money laundering risks associated with onboarding the customer.

The Financial Action Task Force (FATF), the global standard setter in anti-financial crime guidance, outlines the need for KYC in its recommendation on customer due diligence (CDD)[2]. CDD is a core component of the know your customer process, it's used to verify a customer's identity and assess and monitor the customer's risk on an ongoing basis.

What is Transaction Monitoring?

Financial institutions have a regulatory obligation to monitor transactions for suspicious financial activity and report these to the relevant jurisdiction's financial intelligence unit in a timely manner.

Automation capabilities in transaction monitoring systems come in varying degrees of sophistication for process optimization. Advanced solutions can also process massive volumes of transaction data in real-time, while others remain dependent on batch processing after a transaction event has occurred.

Regardless of the type of technology leveraged, firms must adopt a risk-based approach to transaction monitoring and clearly define all the parameters and thresholds that would trigger an investigation, based on their own risk appetite.

A risk-based approach also requires firms to be consistently identifying, assessing, and understanding the financial crime risks present and taking the appropriate mitigation measures, concentrating resources on higher-risk customers.

[2] The FATF, Recommendation 10

Challenges for Fintechs

Combating Data Silos

Unfortunately, fragmented data is common among financial institutions, creating data siloes across an organization. This data is housed in different systems, it becomes clunky, inefficient, and detrimental to overall anti-financial crime efforts. When analysts are forced to move between different platforms and client profiles to piece together information during an assessment or investigation, they lose valuable time and are more prone to error. 100% of fintechs surveyed felt that moving between siloed KYC and transaction monitoring data platforms reduces their ability to assess risk effectively (Figure 2).

To What Extent Do You Agree That Moving Between Siloed KYC and TM Data Platforms Reduces Your Ability to Assess Risk Effectively?

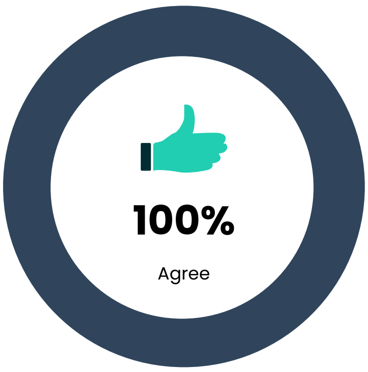

Figure 2

As firms scale, they need to be agile and able to build out their product and service offerings, as well as their compliance framework quickly.

Balancing these goals often results in different teams building out data requirements in order to meet differing priorities. As new financial crime risks emerge, it becomes difficult and inefficient to manage and review customer data stored across disparate systems and processes. This can cause long-term issues with the compliance framework. It not only affects the process of reviewing alerts but also pulling together management information to assess risks and identify problematic clusters of customers. And these issues will persist if not actively remediated.

"It is very difficult to manage risk in an effective manner if your data is in different silos, meaning there is no holistic picture of the customer risk profile."
- Perpetua Gitungo, MLRO & FinCrime Compliance Lead, Wise.

Keeping up with Change

While fintechs are nimble by nature, keeping up with increased regulatory demands is crucial. Scaling effectively requires the ability to offer new products and onboard new customers without sacrificing compliance capability.

As the regulatory environment becomes more stringent, firms must quickly adjust their controls and processes. Only 13% of fintechs surveyed believe their AML workflow could be swiftly configured to new regulatory demands, such as the 6th Anti Money Laundering Directive (6AMLD) or Bank Secrecy Act (BSA) supervisory updates (Figure 3).

How Quickly Does your AML Workflow Configure to New Regulatory Demands?

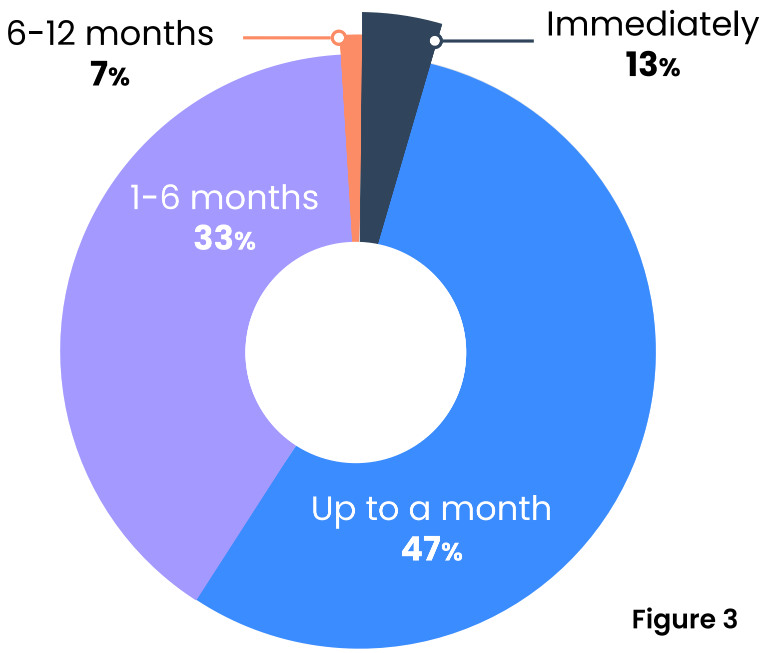

Figure 3

Reducing Customer Friction and Operational Inefficiencies

According to our survey, customer onboarding is one of the top concerns for compliance departments. It's also one of the most important from a customer standpoint. Research has shown an upwards trend in application abandonment in recent years, with 68% of customers abandoning applications in 2022[3].

Finding a balance between effective compliance and a positive customer experience is challenging for all fintechs. Growth is imperative for survival, but potentially opens the business to unwanted financial crime risks. Having the right amount of friction that doesn't negatively impact the customer's journey and result in onboarding drop-off rates is vital.

Balancing compliance with global growth is another issue; one interviewee spoke about the challenges of upholding a standardized customer experience while contending with language differences, document particularities, and other jurisdictional nuances. Focus on customer friction expands beyond onboarding; it also means that customer experience is considered in ongoing monitoring and periodic reviews.

[3] Battle to Onboard 2022

Scaling the Business Sustainably

A key challenge with growth is having the proper infrastructure to support an influx of new customers and activity. Not having capacity planning and human capital can create remedial problems down the line. Firms need to be agile when scaling, and having technology solutions that do not grow with them fast enough creates issues.

One interviewee commented on the rapid growth experienced by their firm, one that their partners had not been expecting, which created problems for their technology infrastructure and diverted their focus during an already busy period. According to Fenergo's survey results, only 40% of fintechs believe that their transaction monitoring system can scale rapidly in response to increasing transaction volumes (Figure 4).

Is Your TM System Able to Rapidly Scale in Response to Increasing Transaction Volumes?

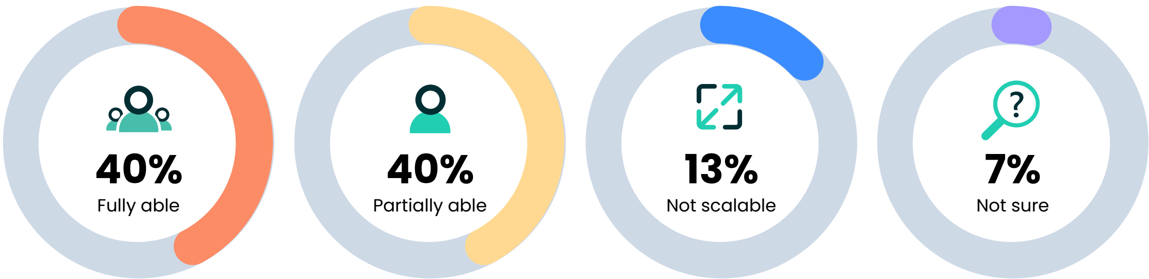

Figure 4

Poor Data Quality

Poor quality data hinders anti-financial crime compliance processes. Often, KYC data is not regularly reviewed and is only refreshed during a periodic review. As a result, KYC data is not in sync with transaction monitoring data and cannot meaningfully support transaction monitoring alerts or investigations.

This lack of synchronicity contributes to the fact that a fifth (20%) of survey respondents have low or no trust in the accuracy of their KYC data when cross-referencing it against transaction data, with only 53% somewhat trusting it (Figure 5).

How Strongly do You Trust the Accuracy of Your KYC Data When Cross-referencing it Against Transaction Data?

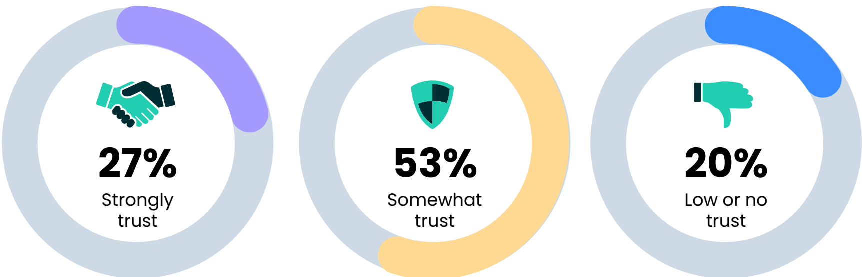

Figure 5

Keeping customer information up to date is a significant challenge for fintechs. Common areas where data changes are:

- Individual financial information, such as income and employment details
- Addresses and contact details
- Beneficial ownership and legal structures

As a result of these changes, the risk profile may also change, which is significant for transaction monitoring as the risk of outdated or inaccurate KYC creates issues that impact client experience and a fintech's capabilities to dynamically manage patterns and typologies of risk.

Making the Case for Integrated KYC and Transaction Monitoring

Fenergo's analysis[4] of regulatory breaches and enforcement actions illustrates the challenges that financial institutions commonly struggle with around KYC and transaction monitoring.

These shortcomings, if unchecked, can manifest into major regulatory violations that lead to heavy fines, bad publicity, loss of trust from customers and investors, and serious damage to the profit margins of small to mid-sized fintechs. All these consequences highlight the existential need for fintechs to address any underlying deficiencies in their compliance practices.

Case One

In an example that points to the failure of a firm's compliance program to keep pace with its growth, an enforcement action was brought against USAA Federal Savings Bank (USAA FSB) in March 2022 for violating the Bank Secrecy Act[6].

USAA FSB allowed millions of dollars linked to suspicious activity to flow through the US financial system, failing to properly report thousands of suspicious transactions.

While the firm's customer base and revenue grew tremendously, it "failed to match that growth with effective AML compliance capabilities". Internal policies, procedures, and controls were deemed insufficient, teams were understaffed, and case alert and investigation systems were chronically deficient.

The Financial Crimes Enforcement Network (FinCEN) fined USAA FSB $140 million, a stark reminder that fintechs need to anticipate growth and scale responsibly.

Case Two

An additional example of failure to achieve safe and sustainable growth comes from Robinhood Crypto, LLC (RHC). The New York Department of Financial Services (NYDFS) found the crypto firm's BSA and AML program to have several issues, including being inadequately staffed and failing to transition from a manual transaction monitoring system that was unsuitable for RHC's size, transaction volumes and customer profiles in a timely manner[7].

The NYDFS stated that RHC did not invest proper resources and attention "to develop and maintain a culture of compliance", especially as the business grew, nor did it maintain "adequate transaction monitoring systems commensurate with its growth".

Not recognizing the need to scale its compliance function resulted in significant AML violations for which RHC paid $30 million in penalties.

The issues experienced by these firms are not unique. They highlight the importance of bringing together customer data to create a more dynamic risk management model and of investing in systems that allow scalability and efficiencies to support growth.

[4] Fenergo
[6] FinCEN
[7] DFS, New York State

KYC and Transaction Monitoring: Getting it Right

In light of the challenges in transaction monitoring and KYC, there are promising and innovative solutions that firms can leverage to alleviate pain points.

Combating Data Silos

Having one platform or 'source of truth' where information is clear, accurate, and accessible.

One interviewee stated the importance of eliminating duplicative customer data points that may be derived from across onboarding, customer service, or transaction monitoring teams, describing the need to take a step back and determine, "What do we need our golden source of data to be? And who should control it?"

Having one clean and central source instead of disparate information flows aids compliance staff in adequately assessing financial crime risk.

"It's rare that a transaction is in and of itself risky based on a single factor. There's risk because of its interaction with various risk factors. The nature of the business often drives those risk factors. What is deemed risky for a specific client may not be deemed risky for another client. But you only know that when you understand the underlying client effectively."
- Dhanush Lodhia, Head of Strategic Execution, ClearBank

An integrated approach with one interface to access is an antidote to data silos. It helps staff glean a more accurate view of the client and any associated risk, enabling better, quicker decision making.

Partnering with a technology vendor to integrate information from different parts of the customer journey, like KYC and transaction monitoring, can massively help compliance teams to review alerts more efficiently, conduct more effective investigations, and compile suspicious activity reports much faster.

Integrating KYC and transaction monitoring data and taking it out of silos can also enable deeper analysis, such as identifying clusters of individuals or financial crime trends. These insights, when fed back into a firm's overall compliance strategy, can facilitate moving from a predominantly reactive anti-financial crime approach to a more proactive, dynamic one.

Keeping up with Change

Those we interviewed stressed the need for in-house compliance experts to translate regulatory changes and champion a clear, pragmatic action plan.

"Hire smartly. If you don't hire the right people, you won't be having the right conversations and the right sort of mentality to think about how you're going to solve problems and scale compliantly. Hire problem solvers because the one thing you won't be short of is challenges."
- Perpetua Gitungo, MLRO & FinCrime Compliance Lead, Wise

Keeping up with the pace of regulatory change is a challenge for already stretched compliance teams at fintechs. Using technology that can rapidly embed new regulatory requirements and adjust customer journeys where necessary is vital. Therefore Fintechs need to work closely with software partners and technology teams to ensure their systems and processes are adaptable.

As one interviewee highlighted, it's important to understand how hard it is for your firm to change existing rules and processes. That knowledge is needed to assess the impact of changes to your teams and to prioritize regulatory change in your technology change cycle with minimal disruption.

"There are so many regulatory changes and considerations. It becomes a question of 'how do we prioritize?' Maximize technology to reduce some of the manual processes and hire experts that are focused on financial crime typologies, or can effectively translate regulations, and make practical changes."
- Patrick Green, Global Head of AML, Banking Circle.

Reducing Customer Friction and Operational Inefficiencies

Having the right tools and technology solutions helps reduce customer friction while upholding compliance obligations.

As one interviewee stated: "There does not need to be a 'tug-of-war' between sales and compliance; ultimately, we are all just trying to get good customers."

Questioning why certain data points are required and how they will be used can help fintechs to determine the value of increasing the complexity and length of the customer journey against the balance of mitigating financial crime risks.

Automatically synchronizing data from transaction monitoring with KYC will further enhance this process and help firms move towards a dynamic model for managing customer risk.

As noted by one interviewee, using advanced technology solutions like artificial intelligence helps fintechs to reduce false positive alerts in transaction monitoring, as behavior-based and pattern-based analysis can more accurately flag or discount potentially suspicious financial activities. This allows for a reduction in manual compliance and associated costs, as well as in unnecessarily flagged alerts and investigations which could lead to customer transaction delays and frustration.

"We decrease manual compliance costs regarding alerts by using machine learning and artificial intelligence. We can process a high number of alerts and help the machine 'learn' based on behaviors or patterns that we assess as being false positives or non-suspicious."
- Patrick Green, Global Head of AML, Banking Circle.

Scaling the Business Sustainably

Fintechs must implement AML workflows and technology solutions that are robust enough to respond to growth.

Part of this is having a contingency plan for unexpected change and keeping the right team and tools on hand.

"I like to think of it as pressure valves. When we have an unexpected growth spurt or when regulations change and you need to change the control environment which requires more resources, we outsource. From a compliance perspective, it helps us move very fast because capacity isn't an issue. It also relieves the pressure on internal teams who can then focus on areas that may require more attention or expertize. Having pressure valves is really key to adapting to changes quickly because we don't have to worry about capacity or compromise the good customer experience."
- Perpetua Gitungo, MLRO & FinCrime Compliance Lead, Wise

When choosing a technology solution to support growth plans, it's essential that fintechs select suitable vendors that can grow with the fintech's business to cater for growth or unexpected volumes.

When selecting a vendor, firms should consider reputation, security, and capabilities, as these factors will help determine if a solution will continue to be a good fit as the business grows. Will the vendor be in business in the future? Will their product still be able to service an increased capacity? These are critical operational risks to consider.

As Dhanush Lodhia, Head of Strategic Execution, ClearBank advised, "as well as anticipating growth, you and your partners need to have built in the capability and capacity to grow in line with the business."

Poor Data Quality

Accurate data is the key to identifying financial crime risk, pinpointing trends, and emerging typologies, and informing the overall anti-financial crime approach.

Incomplete or old data impacts compliance efficiency. Relying on periodic reviews, usually conducted at one-year, three-year, or five-year intervals, can delay a fintech's response to client profile changes. At firms that conduct periodic KYC reviews at set intervals, risk profiles are often inaccurate, exposing the firm to unknown financial crime risks.

"There's two parts to data quality. Firstly, what can you do with the data you've got? Secondly, what do you need to do to improve your data quality in the longer term? You can't do one in the absence of the other. If you're waiting for data quality to be excellent before you do anything, you'll never start. You have to consider what is workable right now. Because fundamentally, you should have some data which is usable. The question is how usable is it? And how do you make it even more usable?"
- Dhanush Lodhia, Head of Strategic Execution, ClearBank

Part of the solution is for fintechs to continuously refresh KYC information through various data points that are trigger or event-based, instead of waiting for a scheduled review to crop up.

Implementing dynamic AML processes makes KYC data more accurate and aids transaction monitoring reviews. Integrating KYC and transaction monitoring systems makes use of your client's existing data continuously to assess risk.

Conclusion

In a world of increasingly stringent regulations, steep noncompliance fines, and evolving financial crime threats, fintechs must find ways to balance their people and technology resources to overcome their biggest compliance challenges without sacrificing other priorities.

Firms within the fintech space must strive to harness technological advancements for compliance processes and leverage their existing data effectively, while striking an optimal balance between human and machine resources to enhance customer experience. Harnessing data intelligently can reduce operational costs, benefit compliance teams' workflows, and lead to operational efficiencies that are essential for a firm's survival.

"Utilize technology. But only utilize technology that is an asset and can truly enhance your program, growth, and customer experience. Because sometimes you can adopt technology and it becomes a burden either in terms of cost or in terms of how long it takes for it to adapt to changes or the false positives it's spitting out."
- Perpetua Gitungo, MLRO & FinCrime Compliance Lead, Wise

Finding smarter ways to use data and technology is therefore paramount. By integrating two of the most important anti-financial crime processes, KYC and transaction monitoring, advanced compliance frameworks can nurture fintechs' growth and support them to scale for success.

Ultimately, the success of all this hinges upon fintechs instilling the right compliance culture across all functions. Otherwise, it won't matter how good your compliance technology is or how well you hire. A culture that doesn't understand the role compliance has to play in achieving profitability goals will undervalue any investment you make in the business.

Transform Client Operations and Compliance with Fenergo

Closing the loop on financial crime by digitalizing and integrating KYC and Transaction Monitoring into a single, SaaS solution.

With Fenergo KYC and Transaction Compliance you can achieve:

- **Real time transaction monitoring**
- **Intelligent KYC policy management**
- **Seamless integration**
- **Continuous monitoring**

To download the brochure visit here or to request a demonstration visit here.

fenergo

For further information
about Fenergo

Visit **www.fenergo.com**

Email us
discover@fenergo.com

FINTRAIL

For further information
about FINTRAIL

Visit **www.fintrail.com**

About Fenergo

Fenergo is the leading provider of Client Lifecycle Management (CLM) solutions that digitally transform how financial institutions, asset management and fintech firms onboard and manage clients throughout their client lifecycle.

Its software digitally orchestrates every client journey from initial Know your Customer (KYC) and client onboarding, automating regulatory compliance and enabling continuous monitoring throughout the client lifecycle (transaction monitoring, perpetual KYC), all the way to client offboarding.

Fenergo is recognized for its in-depth financial services and regulatory expertise and out-of-the-box rules engine which ensures financial institutions are future-proofed against evolving Environmental, Social and Governance (ESG), KYC, Anti-Money-Laundering (AML), tax and prudential regulations across 120+ jurisdictions. Headquartered in Dublin, Ireland, Fenergo has offices in North America, the UK, Poland, Spain, South Africa, Asia Pacific, and the United Arab Emirates.

About FINTRAIL

FINTRAIL is a global consultancy passionate about combating financial crime. We've worked with over 100 global leading banks, fintechs, other financial institutions, RegTechs, startups, venture capital firms and governments to implement industry-leading approaches to combatting money laundering and other financial crimes.

With significant hands-on experience helping scaling fintechs, we help you prepare, assure, and fortify your controls to meet evolving regulatory requirements. Get in touch via https://fintrail.com/contact