Contents

01 Introduction 3

Section 1: The Challenge
02 Managing AML/CTF Risk with Legacy Technology 5
03 The Evolving Regulatory Landscape 5
04 Partnerships and Regulations 7
05 Crypto and CBDCs 7

Section 2: RegTech
06 Existing and Emerging RegTech Solutions 9
07 Domestic vs. International Challenges 11
08 Moving from Manual to Automated Solutions 12
09 Assessing the Impact of New Solutions: By Function 12
10 Assessing the Impact of New Solutions: By Business Type 13

Section 3: Technological Innovation: AI and ML
11 Data is a key source of future opportunity 16

Section 4 Financial Crime
12 Has RegTech impacted the underlying world of Financial Crime? 18
13 Typologies 18
14 Young people are particularly vulnerable 18
15 Crypto crime is creating new challenges 18
16 Conclusion: What does success look like? 20
Introduction

As financial crime typologies, payments use cases, and regulatory technologies continue to evolve, how should compliance teams in remittance and cross-border payment firms build and scale their anti-money laundering (AML) programs?

This is the question we asked leading compliance professionals and industry experts. Their answers have shaped this guide, and the recommendations included in it.

Our conversations showed an industry torn between the potential of artificial intelligence (AI)-driven solutions and the practical challenges of migrating from legacy technologies. Firms are also conscious of the complexity of their payment supply chains and the need to integrate with partners to deliver services.

Organizations must navigate changing regulations and regulator expectations, particularly in the emerging crypto sphere. Cryptocurrencies also raise important privacy questions which have to be credibly addressed.

Put together, the AML compliance picture for remittance and cross-border payments is a complex one. Orchestrating datasets effectively and investing in the right technology, and firms stand to gain new customers and scale successfully. Make the wrong decisions, and organizations risk being left with siloed solutions and frustrated customers.

Each section in this guide explores a different theme related to these challenges and opportunities, from managing AML risks with legacy technologies to the impact of RegTech on financial crime.
Section 1
The Challenge
Managing AML/CTF Risk with Legacy Technology

“There is a need for balance between automation and human intervention for good customer service.”

Mohammad Arslan Naeem, Chief Compliance Officer & MLRO at ACE Money Transfer

New products, fund flows, partnerships, and technology are, together, giving rise to increasingly complex fraud and financial crime typologies. As guidance issued by many regulators indicates, financial crime has increased in many areas - such as ransomware attacks.

Manually delivered regulatory and financial crime risk management regimes struggle to identify many of these attacks, capture the right data to act quickly, mitigate losses and avoid regulatory breaches.

One area where this challenge is evident is transaction monitoring. Traditional systems are based on a static analysis of a predetermined set of risk factors. Updating these systems with new algorithms can help generate more complex risk assessment frameworks. But even with these improvements, achieving real-time transaction risk management may not be possible.

Suppose a legacy system is based on excel or static reporting platforms. In this instance, it is difficult to analyze data at a large scale, impacting the accuracy needed to comply with evolving AML regulations. Indeed, the Financial Action Task Force (FATF) has argued that “the quality of the data obtained by legacy systems varies and may not offer the accuracy and detail required to comply with AML/CFT standards.” Despite these risks, the FATF notes that the “complexities and costs” related to upgrading legacy systems limit innovation in the AML/CFT space. A “real or perceived lack of regulatory incentives to pursue innovation” is a contributing factor.

Another risk comes at the onboarding stage. Banks take, on average, 24 days to onboard customers, which is expected to lengthen with KYC and AML regulations continuing to evolve. With research showing that customers abandon an onboarding process that takes longer than an hour - with more than half doing so if it takes more than 10 minutes - many organizations are losing potential customers at the first hurdle.

The Evolving Regulatory Landscape

“Not only are the AML regulations getting more complex, but there are also other regulatory matters that Compliance Officers need to consider such as safeguarding client funds, internal fraud, and operational resiliency.”

Simon McFeely, Chief Risk & Compliance Officer at TransferMate

Underpinning the evolving regulatory landscape for cross-border payments and remittance firms is guidance from the FATF. It recommends payment services firms use a risk-based approach across their counterparty due diligence regimes, including in their AML/CTF framework, when monitoring transactions. Risk assessments must be carried out continuously to develop an accurate risk profile.

However, regulatory changes such as European Union Directive 2015/2366 (PSD2) make applying a risk-based approach a constant challenge. Designed to harmonize payments across the EU, PSD2 included requirements related to indirect customer due diligence (CDD) and protecting customers from online frauds (strong customer authentication -SCA).
At the enforcement level, the ongoing rise in the sophistication of money laundering and some high-profile cases such as the Wirecard fraud case and various virtual asset-related frauds, are prompting regulators in the US, EU, and globally to introduce reforms aimed at improving how firms in their jurisdictions respond to financial crime.

The European Commission has proposed the creation of an AML/CTF rulebook to act as a guide for regulators and companies. It also proposed several other reforms, including creating a new AML/CFT authority. A new transfer of funds regulation will bring crypto asset service providers (CASPs) into scope. This is designed to tackle the cross-border nature of fund and asset transfers more effectively, ensure the traceability of transactions through the payment chain, and manage ML/TF risks more effectively for the financial sector.

In the UK, the government re-examined its AML regulations in 2021, looking at changes related to compliance with international standards on virtual assets and proliferation financing risk assessments. Additional regulation is expected relating to blockchain transactions and risk assessments during the onboarding process.

The government also initiated reforms calling for reviewing the current money laundering regulations and the Office of Public Body Anti-Money Laundering Supervision Regulations (OPBAS). The main areas of introspection are the approach to risk (how the private sector will identify and control financial crime risk), the structure and scope of the current AML supervisory regime, and the use of technology in compliance. The UK aims to push its agenda forward while taking elements and insight from regimes in the US and EU and integrating them into its strategy.

The changing regulatory landscape adds another layer of complexity to firms' efforts to comply with their AML obligations. Regulatory demands can increase cost and time pressures for international payments. 2-5% of global B2B cross-border payments are subject to additional investigations. Regulators are pressuring firms to contain their misconduct risks, coordinating their efforts across multiple jurisdictions. The Financial Stability Board has even issued a toolkit to help firms reduce their misconduct risks. It breaks the topic down into cultural drivers of misconduct, individual responsibility and accountability, and what it calls the "rolling bad apples" phenomenon.

“We have to adjust to the evolution of regulation and the technology available to us. The technology we use and the way we run our operations need to evolve into the regulatory framework.”

Benjamin Ndubuisi, Product Lead, Ving.ai

Regulators will, broadly, continue to support innovative approaches to compliance, including appropriate co-sourcing/third party arrangements, the adoption of FinTech, and AI. Yet firms’ struggle with data volumes, siloed systems, and data controls have continued.

Even with increased coordination between enforcement bodies, the degree of regulatory change risks further arbitrage. For example, regulators can take different views on what is acceptable when screening transactions. A system alert arising from a calibration issue may not be a problem for some regulators, but others would expect all alerts to be reviewed, regardless of the cause. This makes an agile, dynamic compliance tech stack more critical than ever.
Partnerships and Regulations

Firms must also ensure requirements are enforced across partner relationships. The stakeholders we interviewed told us of the need to provide regulatory reporting to multiple banking partners across different regulatory regimes. However, there was an acknowledgment that technological advances and data reporting can make this process easier.

"I think every company has to follow the same rules, but there are different ways of adhering to them. Compliance is always evolving, so it's about working with partners and ensuring we are on the same page. Partners will always carry out their own compliance, particularly banking partners."

_Compliance Operations Manager & Deputy MLRO, global money transfer service_

Crypto and CBDCs

As consumers and criminals focus on digital currencies, regulators are diverting their attention to areas such as custodian wallets and virtual assets. Evaluating how best to meet Know Your Customer (KYC) requirements in these areas is a particular focus.

The EU, for example, is actively exploring the regulation of cryptocurrencies. In July 2021, the European Commission released a set of legislative proposals that will see the transfer of fund regulations (TFR) extended to all virtual asset service providers in the EU and mandate the collection of information about the senders and recipients of crypto transfers. The UK’s crypto regulatory landscape is expected to stay broadly aligned in the short term.

One area which could have particular significance from a regulatory perspective is Central Bank Digital Currencies (CBDCs). Wider adoption of CBDCs would lead to questions around privacy and regulation, given the risks posed by anonymized virtual asset networks.

As with regulatory changes more widely, payment firms should prepare to manage arbitrage, particularly concerning cross-border payments.

Payment services firms will likely need to manage regulatory differences between jurisdictions. Firms should keep up with statements, consultations, and draft legislative proposals issued by policymakers in their jurisdictions and act accordingly.
Section 2

RegTech
Existing and Emerging RegTech Solutions

Financial crime and its detection are growing markets. One leading driver of this is the increasing quantity of transactions. In the UK alone, payment volumes are forecast to increase from 39.3bn in 2018 to 43.3bn by 2028. An even greater rate of change can be expected in countries with higher financial crime risks.

“With remittance, a big challenge is knowing where the funds came from and where they go to. Proving identity is the biggest issue. This is very different from other markets, such as card payments. The remittance market is ripe for challengers to enter it.”

James Lynn, Co-Founder, Currensea

Much of today’s security tech infrastructure consists of legacy systems. These systems rely heavily on human input, creating inefficiencies and inaccuracies that impair not just the customer due diligence process but the financial security of firms as a whole. Some estimates have suggested that false positives account for 42% of all AML alerts.

Other issues relate to the cost of modernization and the limited levels of technology expertise and awareness among AML professionals.

These challenges pressure the overarching customer due diligence (CDD) framework that remittance firms must build and iterate. As a result, many are turning to RegTech solutions to manage evolving risk profiles, automate and triage alerts and improve scalability. This can also help prioritize in-house compliance expertise on the most challenging, urgent, and high-risk issues. RegTech firms evolve and improve their products, and regulators’ expectations change, too. As a result, many firms realize innovative RegTech is critical to achieving scalability.

RegTech isn’t just important for regulators. Many remittance and international payments firms will work with partners such as correspondent banks, meaning that an end-to-end cross-border solution is often an aggregated solution delivered by multiple providers. Success across this complex chain requires automation, and the expectation at a peer-to-peer level is high. Firms must show their solutions are interoperable - for example, through compatibility with global card scheme standards.

However, emerging RegTech solutions do not fit into a “catch-all” bucket. For comprehensive AML/CFT compliance, firms need to review several areas of their RegTech stack:

ID Verification (IDV)

Innovation in ID verification has been accelerated by the pandemic, and firms have now started using biometric authentication measures, such as selfies, fingerprints, or voice recognition measures to make the onboarding process more efficient. For example, analysts like Gartner have noted a growing trend toward digital ID wallets for citizens, enabling them to disclose identity-related data while giving consumers greater control and privacy. The European Commission has also suggested using digital ID wallets to access services.
Screening for Sanctions, PEPs, and Adverse Media

In addition to IDV, firms need to ensure they are managing their exposure to sanctions risks by screening customers against relevant lists at onboarding, and on an ongoing basis, in alignment with the firm’s risk-based approach. Russia’s invasion of Ukraine in February 2022 highlighted the speed at which sanctions lists can change and the importance of real-time monitoring for potential sanctions exposure.

Customers identified as **politically exposed persons (PEPs)** will require additional due diligence. Again, however, PEP classifications can change quickly, and individuals can acquire or lose PEP status in a short period of time. Screening requirements differ globally too. The United States, for example, does not require domestic PEP screening.

Sanctions lists also only capture individuals and entities already identified as high-risk. Remittance firms should use adverse media screening systems for comprehensive coverage, ensuring they capture not only designated persons but also potential “cut-outs” or proxies that could be used to evade sanctions. Adverse media can greatly enrich a firm’s data and help identify these less visible risks. This is especially critical for enhanced due diligence (EDD).

“Once someone is onboard, we use several tools in the background to verify ID and check against any watchlists. So we check to see if they are who they say they are, or if any negative news flags up, and depending on the location, our onboarding usually takes less than 24 hours.”

**Chief Strategy Officer**, global payment processor

Transaction Monitoring

Firms that use rule-based systems to monitor transactions can only detect suspicious behavior based on known and existing scenarios. This became worse with the pandemic, as new predicate offenses emerged, resulting in risk assessments quickly becoming outdated.

Effective transaction monitoring also depends on the data it captures, and rule-based transaction monitoring systems may not generate accurate risk profiles. Firms also face challenges in terms of regulatory compliance and operational processing.

Automated, risk-based transaction monitoring frameworks help firms keep pace with the evolving financial crime market and allow data to be processed comprehensively, with speed and accuracy that manual compliance processes could never achieve. **AI and machine learning** can make the onboarding process smoother by accurately flagging and rectifying false positive alerts and adapting to regulatory changes and jurisdictional disparities.

“Automation has made transaction monitoring and payment screening efficient and effective. There is more accountability and traceability online.”

**Mohammad Arslan Naeem**, Chief Compliance Officer & MLRO at ACE Money Transfer
**Crypto**

New planned EU regulations for the virtual asset service provider (VASPs) sector provide just one example of why crypto is an area where regulatory technology in general - and transaction monitoring systems in particular - are becoming crucial. Even VASPs not required to onboard this technology for their operations may find it an essential requirement for the partnerships needed to support off/on ramps between crypto and fiat currencies. As new regulatory frameworks confirm, VASPs do not operate in a silo. Intersecting with fiat currencies and the regulated entities that serve those currencies will require an investment in RegTech.

It’s also important to remember that deploying RegTech solutions doesn’t negate the need for experienced compliance staff. Rather, the nature of the hires firms make will change. Talented, experienced individuals are needed to deploy tools, manage their outputs, and make decisions based on the alerts they generate. Over time, this may lead to firms offering fewer entry-level, functionary jobs, with a leaner, more experienced team focused on higher-risk activities. However, these teams still need to be ready to scale with their organizations.

**Reporting**

**Internal** - For internal risk assessments, it’s important to remember that financial crime is just one part of a firm’s wider enterprise risk assessment. Many helpful tools are available to support teams conducting these reviews, such as those offered by the [International Compliance Association](https://www.icaglobal.org). Other considerations will be invoice tax reporting obligations and ISO standards.

**External** - Areas like tax compliance can also become external considerations. In the United States, for example, firms must report on customer tax IDs. Similar nuanced obligations exist around the world. Firms must also ensure they’re capturing and reporting transactions according to the thresholds defined in their jurisdictions.

**Domestic vs. International Challenges**

Financial institutions on the SWIFT network can send and receive transaction information in a standardized way. These transactions can occur anywhere in the world and any currency. While SWIFT is traditionally a messaging service, it is increasingly evolving to become a transaction management platform.

Encouragingly, 95% of payments through SWIFT can now transfer from one beneficiary to the other within 24 hours of the transaction taking place.

However, most payments firms are not banks. They operate outside the SWIFT system and seek to lower costs by delivering solutions that don’t rely on SWIFT services. The costs associated with SWIFT are tough to justify for lower value and volume payments. Domestic solutions to this challenge have proven harder to scale internationally. As a result, the current marketplace of options is crowded and likely to be consolidated as new standards are introduced.
Some new initiatives are aiming to change the global payments infrastructure. One example is P27, a joint initiative between several banks across the Nordics to create the world’s first real-time, cross-border payment system in multiple currencies. Real-time payment infrastructure is already in place between Singapore and Thailand and should be introduced between Singapore and Malaysia by the end of 2022. Meanwhile, the European Payments Initiative aims to create the world’s first real-time, multi-currency cross-border infrastructure through a consortium of credit institutions and acquirers. It is developing a pan-European payment solution for instant payments and cards, focusing on retail and P2P payments between individuals.

The scalability of some AML compliance tools is greater than others. Transaction monitoring solutions can scale more easily than IDV. The requirements for ID verification vary nationally, applying FATF standards within a particular local context. Greater standardization - either through regulatory change or the commercial success of a particular approach - will be required to improve the efficiency of remittance and international payments.

As a result, firms need to consider where and how they invest in automation and solutions using advanced technologies early in their development. Invest too much too early, and it becomes hard to offer competitive pricing and grow. Spent too little, and firms won’t have the right standards to grow quickly. This is especially key for payments/remittance, where volume is often key to commercial success. Compliance teams need to ensure they are connected to and involved in these commercial considerations and can evaluate products will this approach in mind.

Moving from Manual to Automated Solutions

When and how to move from manual to automated solutions must be informed by a firm's risk-based approach. There is no “one size fits all” answer. Remittance firms should account for:

- Structuring and organizing data sets, especially if these are currently hosted in static database reporting platforms
- Establishing appropriate sandbox environments to ensure any new automated programs are fully tested before being deployed. Firms may also wish to roll out new solutions one line of business at a time, minimizing the impact of potential threshold adjustments and other changes
- Regularly communicating with partners to ensure the migration and any new platforms don’t compromise contractual commitments such as Service Level Agreements (SLAs)
- Instituting a process for monitoring the overall risk profile of an entity and its activities on an ongoing basis. This can change based on internal factors such as ownership, PEPs onboarded, business objectives, and external factors including regulation, jurisdiction, and competition
- Regulators will expect remittance firms to take a “continuous improvement” approach. This means continually reviewing existing models and assumptions and adjusting or redefining these as financial crime risks and criminal behavior evolve

Assessing the Impact of New Solutions: By Function

Any decision to invest in new technology can have both positive and negative impacts on the way a firm functions. As a result, it’s critical to understand and analyze the potential implications before deciding to proceed. This section explores some of the areas payments, and remittance firms should consider by core business function area.

Above all, firms need to remember that there is no one-size-fits-all solution. Compliance teams must identify and implement the appropriate AML processes for their business models and strategies, considering manual and automated approaches and their wider risk appetite.
As highlighted earlier in this guide, when assessing new solutions from a business perspective, firms need to consider the point at which an investment could hinder growth by introducing prohibitively high costs. In making this assessment, firms should ensure they’re assessing the potential costs and benefits on a medium-to-long-term horizon. Investing early in what will become foundational tools makes good business sense, helping companies scale seamlessly and reducing the risk of duplicate work or significant manual remediation efforts.

**Products and Services**

If a firm’s CDD process is comprehensive and well implemented, it should scale with the product roadmap without extensive adjustments. The key to making this happen is onboarding. Onboarding the right customers not only ensures that firms are minimizing their risk exposure. Firms we spoke to also highlighted that suitable customers are versatile and adapt to new products as they launch.

However, remittance firms need to ensure sufficient flex in their CDD process and risk matrix to account for jurisdictional differences. This will be much easier if the process is grounded in principles rather than a specific vendor or process.

**Regulators and Law enforcement**

The challenge faced by many firms around managing the volume and variety of outputs from RegTech solutions is also common to regulators. While regulators are increasingly looking toward intelligence and information sharing to improve financial crime risk detection, they inevitably have standardized processes for the expected outputs.

“There are niche markets with money services businesses. One of the key points to remember is that to regulators, and the FCA in particular, any transaction monitoring should be proportional to your business.”

Head of Financial Crime & MLRO, international FX organization

**Assessing the Impact of New Solutions: By Business Type**

The impact of RegTech solutions will also vary based on business type - this includes the jurisdiction(s) they operate in, the size of their firm, and the demographics of their customer base.
Domestic vs. International

As we've highlighted in this report, implementing new RegTech solutions at the country level is much easier than meeting the interoperability requirements necessary for cross-border growth. As a result, firms should look for best-in-class products that integrate with partners and other vendors involved in the payment process.

It's also important for firms to research and understand the characteristics of new jurisdictions to account for local nuances. This is especially notable in areas like IDV, where the required verification documents will vary substantially from country to country.

Small vs. Large Firms

FinTech-led entrants in remittance and cross-border payments are bringing fast, low cost and customer-led propositions to market and drawing contrasts with established players as they do so.

However, many of these new entrants need to scale up their businesses before fully exploiting the benefits of new technologies. Their ability to invest in deploying capabilities such as AI and ML in remittance activities is limited at the startup stage.

Meanwhile, incumbent organizations may embrace technology to enhance their operational efficiency but face legacy challenges relating to their business models, technology infrastructure, and risk appetite.

As a result, no clear set of firms holds a distinct advantage in the remittance and cross-border payments market. Rather, larger and smaller firms have specific compliance risks and opportunities to manage in line with their risk appetites.

Younger vs. Older Customers

Financial services firms, including money transfer businesses, are improving their onboarding processes and other digital systems to suit their younger customers. This includes embracing new technologies that streamline onboarding, and technology that can enable an enhanced customer experience to be delivered, often via mobile apps.

Insight from stakeholder interviews, however, indicated the older population typically feels more comfortable with the traditional onboarding process and less trusting of newer processes such as the use of selfies for identification verification.

These challenges indicate that although the general direction of travel is towards branchless digital onboarding, firms need to be mindful of not inadvertently withdrawing access to financial services to older customers. Rather, the shift to a tech-led onboarding process must be carefully managed, with appropriate support offered to older customers as needed.
Section 3

Technological Innovation: AI and ML
Advancements in technology can help firms and regulators as they seek to keep ahead of the growing diversity and complexity of financial crime.

Firms are using technologies to innovate to tackle financial crime, including AI and ML, blockchain, biometrics, predictive analytics, and Application Programming Interfaces (APIs).

Underlying many of these innovations is automation. This can make AML processes less time-consuming for compliance professionals within firms while allowing them to flag high-risk behaviors and patterns more accurately. Experienced analysts can then focus their time more where it is most needed.

The growing digitization of the financial services industry is also shifting the guidance regulators provide. Traditional cash-heavy indicators and physical document verification controls are becoming less relevant in the face of digital transactions.

For example, the FCA revised its 5-year data strategy in 2020, focusing on embracing new technologies and making them more accessible. Work is ongoing on a data collection platform to replace the FCA’s existing Gabriel program, alongside exploring digital reporting in partnership with the Bank of England.

One area of opportunity is data sharing, particularly in the context of regulatory reporting and the creation of audit trails. Collaboration among financial institutions is increasing in the fight against financial crime, to the extent that firms may now choose to share insights on AML model performance and use results from multiple financial institutions to fine-tune and optimize their models.

Data is a key source of future opportunity

Due to the increasing volume of criminal activity, manual investigations have become inefficient and sometimes inaccurate. Payments and remittance firms are turning to AI-based solutions to address these challenges while better meeting customer needs and driving efficiencies.

A report from SAS, KPMG, and the Association of Certified Anti-Money Laundering Specialists (ACAMS) surveyed 850 ACAMS members worldwide about their organizations’ use of AI or ML technology to detect money laundering. According to the study, 57% of respondents have either already incorporated or plan to incorporate AI and ML technologies in their AML compliance processes in the next 12-18 months.

According to the report, 28% of large financial institutions (assets greater than $1bn) and 16% of smaller financial institutions (assets less than $1bn) view themselves as innovators and industry leaders in integrating AI and ML into their processes.

These results help to demonstrate that an AI-driven, algorithmic approach can help compliance teams to generate complex risk assessment frameworks, map against a host of potential risks, and identify connected persons and entities. An individual's behavior on its own may not look suspicious but could be flagged for further investigation if connected individuals can be identified to demonstrate a pattern.

“Transaction monitoring needs to be regularly adjusted to protect against fraudsters. We are using a rules-based approach, which can include an automatic acceptance, a manual review, or an automatic rejection when abnormal or fraudulent transactions are determined based on trends. These rules can be adjusted to meet changing trends.”

Maja Chaińska, Head of Compliance, Azimo
Section 4
Financial Crime
Has RegTech impacted the underlying world of Financial Crime?

The intersection of RegTech and financial crime is often shaped by the competing demands of speed and risk. How quickly can a firm onboard a customer without accepting an intolerably high-risk burden? From pandemic fraud to the rise of crypto, the shifting typological sands of the last few months have shown that balancing the demands of speed and risk is an ongoing challenge.

Typologies

COVID fraud

COVID has led to significant changes in consumer behavior and buying habits. FATF members report that criminals have attempted to profit from the pandemic through increased fraudulent activities.

“We’re never one step ahead of the criminals. We’re always trying to catch up until we can work together with the private and public sectors and develop better ways to catch them.”

Nadja van der Veer, Compliance Director, Rewire EU

Online fraud has risen by a third since the pandemic’s start, with £2.3bn lost in 2021. There were also almost 15,000 impersonation scams reported by UK Finance members between January and June 2020, an increase of 84% compared to last year. Most of these cases involved criminals impersonating the police, a bank, or other trusted organizations such as a utility company, communications service provider, or government department. Despite the significant rise in cases reported, the amount lost to impersonation scams over the same period increased by just 3% from the previous year, reaching £58m.

Young people are particularly vulnerable

Industry experts we spoke to told us that young people are increasingly targeted by fraudsters concerning international money transfers and are more vulnerable to getting involved in this activity than older people, especially in relation to money mules. This is an increasing area of focus for compliance professionals in cross-border payments and remittances.

“We see many typologies. Money mules are an emerging trend, as people are under more financial strain. It might be challenging to verify the user’s validity, especially in identity theft cases using stolen cards. A robust transaction monitoring system and technical tools support us in managing this risk.”

Maja Chańska, Head of Compliance, Azimo

Data from fraud prevention organization CIFAS on the overall financial sector indicates a rise in teenage money mules over the last two years. Its data shows a 78% increase in money mule activities in accounts owned by those under 21. It also showed a 76% increase in those aged 21-30 and a 26% increase in those owned by people over 30.

Crypto crime is creating new challenges

Cryptocurrency-based crime is also on the rise, with illegal addresses receiving $14bn in 2021, almost double the $7.8bn reported in 2020. An increase in crypto-based crimes is expected as total crypto transaction volumes increase to $15.8tn in 2021, an increase of 567% from 2020. Many cryptocurrency transactions are tough to track back to the beneficial owner.
“Remittance could face huge challenges with cryptocurrencies. This is partly due to the inherent workload caused by all the intermediaries in the heritage systems we have. The future is disintermediated to align with a cost-effective crypto vision.”

**MLRO & Compliance Officer, International Foreign Exchange Company**

Crypto regulatory frameworks are still being developed globally, varying and often contradicting from country to country.

The EU is actively exploring the regulation of cryptocurrencies. In July 2021, the European Commission released a set of legislative proposals that will see the transfer of fund regulations (TFR) extended to all virtual asset service providers in the EU and mandate the collection of information about the senders and recipients of crypto transfers. The UK’s crypto regulations are expected to stay broadly consistent with the EU in the short term.

As criminals focus more on digital currencies, regulators and compliance teams are also diverting their attention to areas such as custodian wallets, fiat currencies, virtual assets, and prepaid cards. Evaluating how best to meet KYC requirements is a particular area of focus. At the same time, newer ML and AI systems are being used to detect transactional behavior and analyze patterns in cryptocurrency activity.
Conclusion: What does success look like?

Throughout this guide, we’ve explored a host of AML and financial crime compliance best practices for firms operating in the remittance and cross-border payments markets. To summarize what we’ve discussed, we’ve developed this financial crime risk management success matrix, which captures the key areas firms need to consider when assessing their compliance program’s health.

**Operating license**

Remittance firms should consider licensing in two separate ways:

1. Regulatory authorization: The baseline approval firms require to operate in specific jurisdictions, for which automation will be an expectation
2. Marketplace trust: Customers and partner relations are also critical to success. Partners will assess firms for the security of their processes and technology - simply scalability. Some customers are also increasingly able to identify gaps and weaknesses in controls and may go elsewhere if unconvinced.

**Cost control**

Incremental financial crime regulation is adding significantly to the costs financial institutions must bear, driving a need for solutions that reduce costs without compromising on risk management and regulatory compliance. Consequently, firms are investing in technology-enabled controls and compliance processes. However, many financial crime risk management processes and systems still require significant manual effort.

Regulatory pressures can increase the cost and time for international payments. Between 2-5% of global B2B cross-border payments are subject to additional investigations, driving the cost and times of payments.

**Reputational strength**

Firms can also think about their reputational strength in two ways: push and pull factors. For pull factors, they should review the proportion of customers who complete the onboarding process - most likely the key area where compliance and customer satisfaction intersect. For push factors, the wider reputational position of the business matters - e.g., any negative news coverage related to regulatory enforcement action or criminal activity facilitated through a firm.

**Ability to scale**

Do compliance tools provide a platform for growth, or are they inhibitors? Does the compliance organization have the right staff and strong relationships with regulators? All of these factors are key to a firm’s ability to scale - both practically and to attract investment.

**Launching new products**

Compliance controls should not inhibit the development of new products. Rather, new products should align with existing approaches if focused on principles vs. tactics and tools. The involvement of compliance teams in new product launches is a good test of this approach.

**Efficient operations**

As explored in this paper, efficiency through automation requires a balance between speed and scalability. Implemented effectively, automation assistants transparency, scalability, reliability, and - if the technology is right - adaptability. Firms should continually evaluate this efficiency balance as they grow and act to remediate issues as needed.
About ComplyAdvantage

ComplyAdvantage is the financial industry’s leading source of AI-driven financial crime risk data and detection technology. ComplyAdvantage’s mission is to neutralize the risk of money laundering, terrorist financing, corruption, and other financial crime. More than 500 enterprises in 75 countries rely on ComplyAdvantage to understand the risk of who they’re doing business with through the world’s only global, real-time database of people and companies. The company actively identifies tens of thousands of risk events from millions of structured and unstructured data points every single day. ComplyAdvantage has four global hubs located in New York, London, Singapore and Cluj-Napoca and is backed by Ontario Teachers’, Index Ventures and Balderton Capital. Learn more at:

complyadvantage.com

Our Customers

Get in Touch

<table>
<thead>
<tr>
<th>EMEA</th>
<th>AMER</th>
<th>APAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>London</td>
<td>New York</td>
<td>Singapore</td>
</tr>
<tr>
<td>+44 20 7834 0252</td>
<td>+1 (646) 844 0841</td>
<td>+65 6304 3069</td>
</tr>
<tr>
<td><a href="#">Demo Request</a></td>
<td><a href="#">Demo Request</a></td>
<td><a href="#">Demo Request</a></td>
</tr>
</tbody>
</table>
Disclaimer: This is for general information only. The information presented does not constitute legal advice. ComplyAdvantage accepts no responsibility for any information contained herein and disclaims and excludes any liability in respect of the contents or for action taken based on this information.

For details on the source materials used in this guide, please visit complyadvantage.com/insights