KROLL

Fraud and Financial Crime Report

Can technology stop the threat of economic, crypto and ESG crimes?

2023

Foreword

Kroll's 2023 *Fraud and Financial Crime Report* shares the findings from a survey of 400 executives across the globe conducted in Q1 2023. This report navigates the complex, innovative and ever-changing landscape of financial crime and technology and shines light on the more than USD 800 billion laundered every year.

We began 2023 with ongoing economic pressures, geopolitical tensions, an increasingly diverse regulatory environment and exciting advancements in AI. International headlines were dominated by revelations of Ponzi schemes, government scandals, public corruption, greenwashing, sanctions evasion and other economic crimes. Behind these headlines were passionate prosecutors, attorneys, law enforcement officials, regulators, compliance officers and risk analysts working together to combat the rising tide of financial crime. A better understanding of the state of the fight against financial crime has become more important as new technology unfolds.

Our survey found that most companies anticipate an increase in financial crime risks over the next 12 months and have doubts about the capacity of governments to keep pace with technological change and the increase of criminal activity. To close this gap, more than two-thirds of respondents said they were prioritizing their own technology investments. Questions remain regarding how these investments should be made and what else can be done to combat financial crime. This year's report approaches these questions through a combination of survey results and expert commentary from Kroll's global risk experts, focusing on anti–money laundering (AML), anti-bribery and corruption (ABC), sanctions, cryptocurrency and environmental, social and governance (ESG).

This year's respondents represent eight countries including the U.S., the UK, France, Germany, Brazil, Mexico, Singapore and the UAE, with the vast majority working in highly regulated industries. Based on respondent insights, this report individually analyzes results at macro and micro levels and demonstrates a broad spectrum of geographies, challenges and Kroll expertise.

Key Findings

Financial crime continues to be a leading threat globally: Sixty-nine percent of global executives and risk professionals surveyed expect crime risks to increase over the next 12 months with cybersecurity and data breaches as the primary drivers, followed by financial pressures on organizations. In the face of this dynamically evolving landscape, the role of the compliance function remains more crucial than ever.

Organizations are keen to prepare themselves for new and evolving risks: Investments in technology, increase in cybersecurity budgets and undertaking more frequent business risk assessments have been cited by respondents as the three main steps that firms intend to take during the next year to combat the increase in financial crime.

Responding to risk by investing in advanced technologies is a priority: To counter a potential uptick in financial crime risks, two-thirds of respondents globally are planning to invest more in technology, with nearly half of respondents citing data integrity as the biggest challenge when implementing new technologies.

Governments are stepping in with increased measures against financial crime: Globally, the anticipation of increased enforcement actions is on the rise, with over 60% of survey respondents predicting an escalation in the next 12 months. Many speculate that regulatory visits will start looking more closely at the use of technology as part of firms' AML compliance programs. Respondents agree that rapidly evolving technology is the top struggle governments face against financial crime, indicating that governments may face an uphill battle.

AML and ABC functions need to work hand in hand: AML and ABC functions are distinct specializations within most financial crime compliance programs; however, they travel in the same direction and utilize similar tools, methodologies and trainings. Efficiencies can be gained when organizations intentionally seek integration by leveraging shared resources for investigations, audits and risk assessments.

Corporations that are noncompliant face immense financial and reputational consequences: Navigating the complex world of sanctions compliance is a significant challenge for multinational corporations. Forty-four percent of respondents identified geographic consistency as the top challenge for sanctions compliance programs, followed by privacy protections (39%), keeping current with changing regulations (34%) and accessibility of technological solutions to support sanctions screening (33%).

Organizations believe that ESG and transparency are crucial but face procedural challenges: The recurrent theme of balancing transparency and privacy, notably in beneficial ownership, calls for cautious navigation. Likewise, in ESG reporting, businesses must align with evolving standards to avoid the pitfalls of greenwashing and fraud.

Thank you for spending time to review these results, and as always, Kroll is available to further discuss the details of these findings and to partner with you in improving your financial crime compliance, readiness and program objectives.

Meet Our Experts

Haydn Jones
Managing Director and
Global Head of Blockchain
and Cryptocurrency Solutions
+44 780 243 8892
haydn.jones@kroll.com

Chris DeSa
Managing Director
+1 213 443 6052
chris.desa@kroll.com

Julianne Recine
Managing Director
+1 212 871 7524
julianne.recine@kroll.com

Michael Watt
Managing Director
+1 305 428 3393
mwatt@kroll.com

Ned Kulakowski
Associate Managing Director
+1 212 202 5884
ned.kulakowski@kroll.com

Holly Noonan
Associate Manager
+1 617 378 9424
holly.noonan@kroll.com

David Lewis
Managing Director and
Global Head of AML Advisory
+33 7 84 24 14 09
dlewis@kroll.com

Howie Epstein
Managing Director
+1 212 523 0308
howie.epstein@kroll.com

Jordan Strauss
Managing Director
+1 215 568 8238
jordan.strauss@kroll.com

Veronique Foulon
Associate Managing Director
+44 207 029 5155
veronique.foulon@kroll.com

Maria Evstropova
Director
+44 207 089 0861
maria.evstropova@kroll.com

Carolina Attili
Senior Associate
+44 207 089 4927
carolina.attili@kroll.com

Giles Derry
President, Governance
and Risk Advisory
+44 203 405 7980
giles.derry@kroll.com

Jonathan Campbell
Director of Sales
Governance and Risk Advisory
+44 750 012 7809
jonathan.campbell@kroll.com

Jason Smolanoff
President, Cyber Risk
+1 213 700 4312
jason.smolanoff@kroll.com

Darren Hill
Vice President of Sales
Resolver
+1 416 889 3853
darren.hill@kroll.com

Table of Contents


EURO
NOTE
UNITED STATES
OF AMERICA

How Technology is Transforming AML

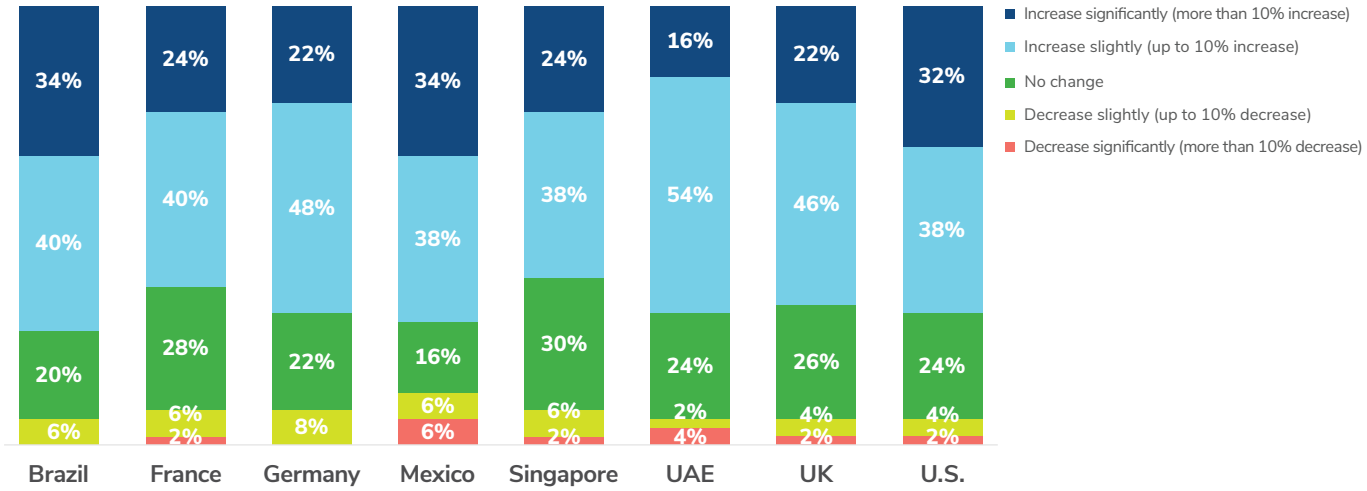
by David Lewis, Ned Kulakowski, Maria Evstropova and Carolina Attili

It is fair to say that the past four years have been challenging: Brexit, the COVID-19 pandemic, economic recession, unprecedented inflation and the war in Ukraine. Each of these events has paved the way for an uptick in criminal activity. The UK's departure from the EU has resulted in a change in international trading relationships, providing more opportunities to criminals in countries that are more vulnerable to corruption. The COVID-19 pandemic has led to global supply chain challenges and an increase in scams, fraud and cybercrime. Moreover, the unprecedented nature of sanctions imposed against Russia has led to firms becoming vulnerable to the risk of providing services to sanctioned individuals or facilitating a transaction designed to circumvent sanctions. The list of reasons for increased financial crime risks is endless.

While financial crime is very often invisible, making it hard to identify, measure and fight, its impact is felt in many ways and affects individuals, communities, countries and businesses around the world. Governments introduce legislation and regulations to fight financial crime and rely on financial institutions (FIs), lawyers, accountants, estate agents, gambling firms and cryptocurrency exchanges—to name a few—to act as the gatekeepers of the financial system. As criminals often target FIs to act as facilitators in the perpetration of crimes, there is significant pressure on the financial services industry to put in place systems and controls which can detect and, most importantly, prevent financial crime.

Half of all participants surveyed are currently employed in the financial services industry. The survey revealed that 69% of respondents globally expected financial crime risk to increase over the next 12 months with a split between 26% expecting financial crime risks to increase significantly and 43% expecting financial crime risks to only increase slightly.

Sixty-Nine Percent of Global Respondents Expect Financial Crime Risks to Increase Over the Next 12 Months

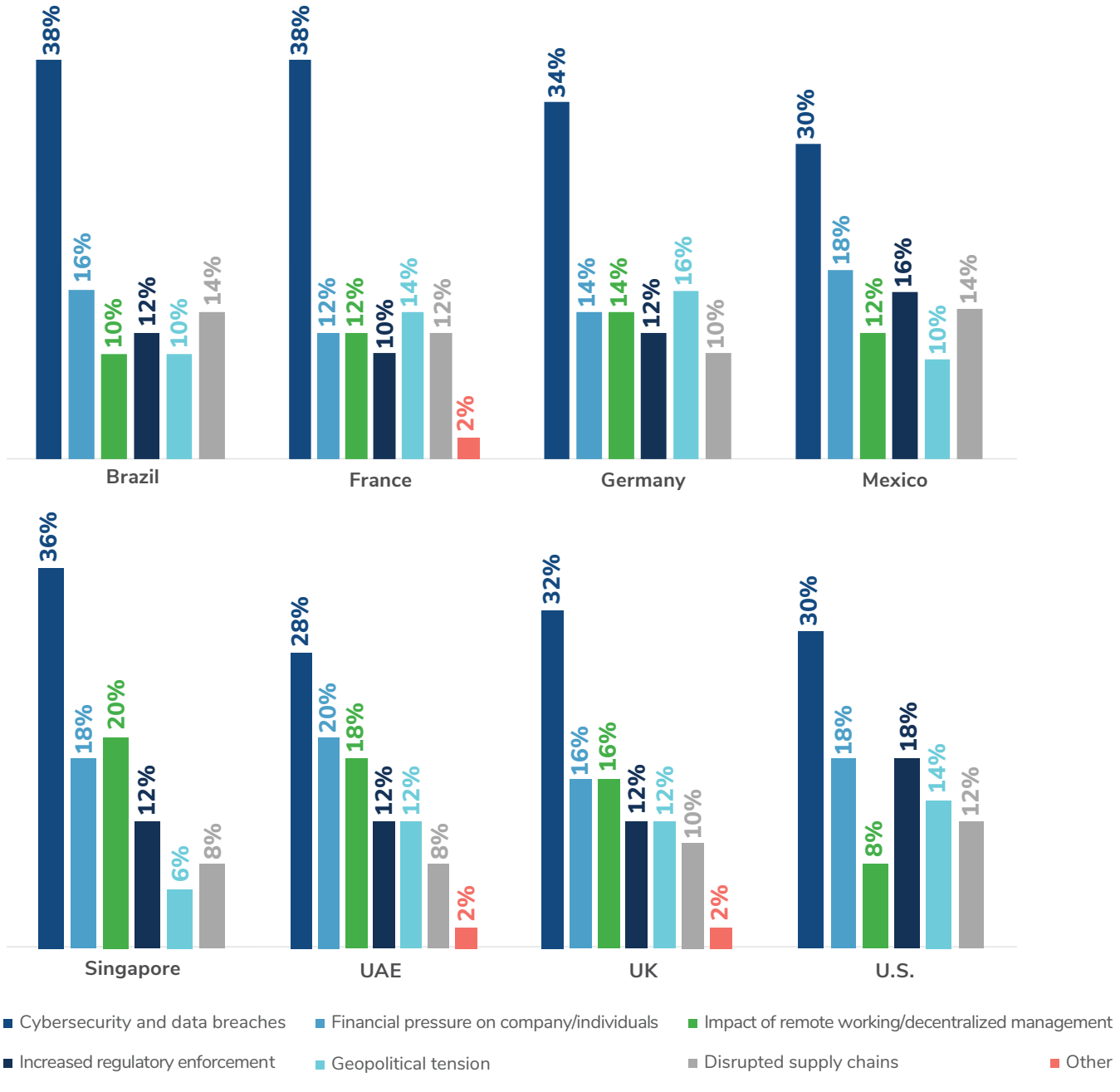


Additionally, respondents cited cybersecurity and data breaches as the main factors behind the increase in financial crime risk. It is not surprising given the growing diversity, complexity and volume of attacks, amplified by ongoing geopolitical tensions and the additional challenge of hybrid work environments post the COVID-19 pandemic.

Losing Ground in the Fight Against Financial Crime

Despite the increase in financial crime globally, it feels that regulators around the world are constantly playing a catch-up game and, ultimately, criminals are always a step ahead. In fact, more than half cite evolving technologies, digital currencies, data privacy and geopolitical tensions as challenges posed to governments in fighting financial crime.

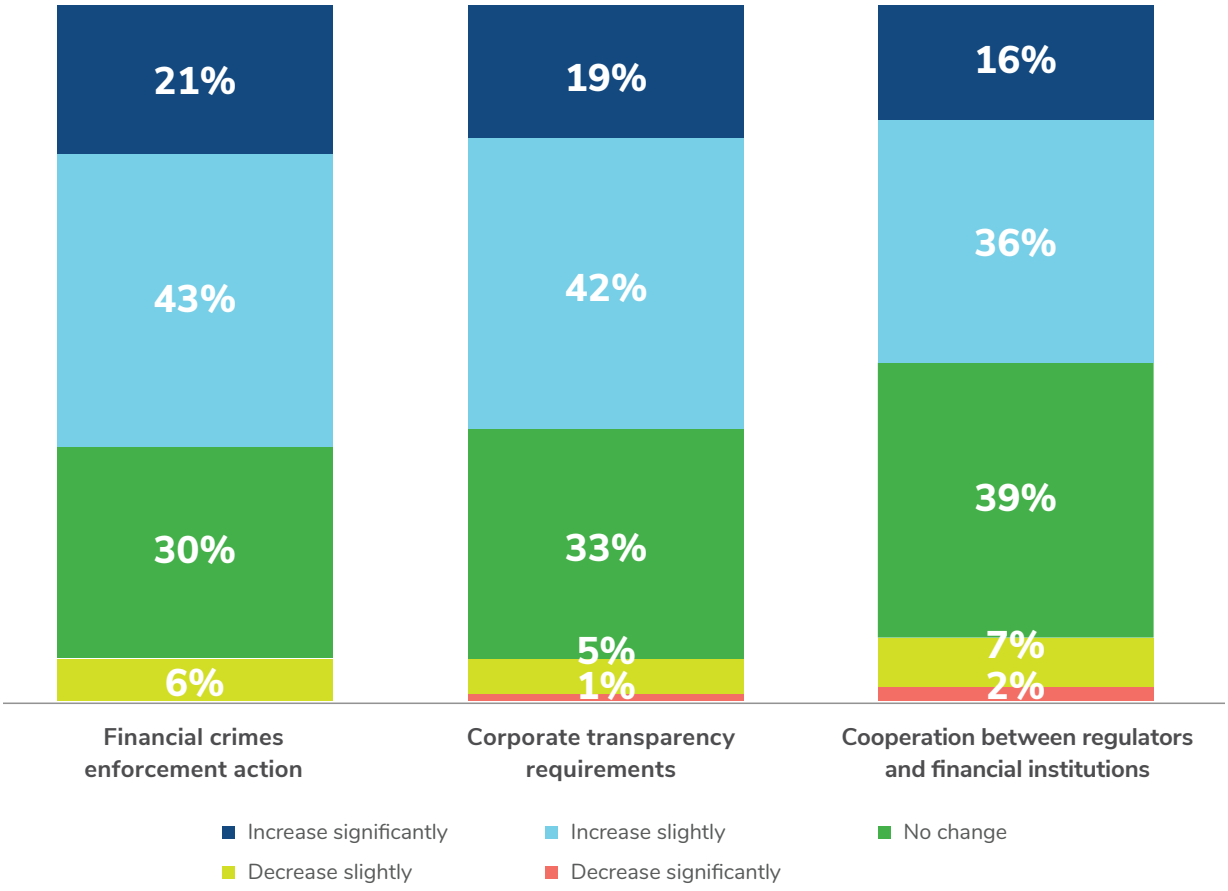
Which Factors are Responsible for the Increased Financial Crime Risk?



We have seen in recent years an increase in collaboration between regulators and both the private and public sectors in the fight against financial crime. However, much more needs to be done to allow firms to share information amongst each other. Existing laws prevent cross-industry and cross-firm information sharing and, therefore, act as a blocker against this fight. Furthermore, certain countries are notorious for being quite secretive and not allowing any information sharing outside of their virtual borders.

Most survey responders felt that, in the next 12 months, the level of cooperation between regulators and FIs will not produce as much fruit as one would hope. However, 64% felt that the level of enforcement actions will continue to rise. Over the years, we have seen numerous enforcement actions against FIs; in some cases, multiple fines were issued against the same FI, and yet the level of crime increases, and the strength of systems, controls and processes is not enough to act as a credible deterrent against criminals.

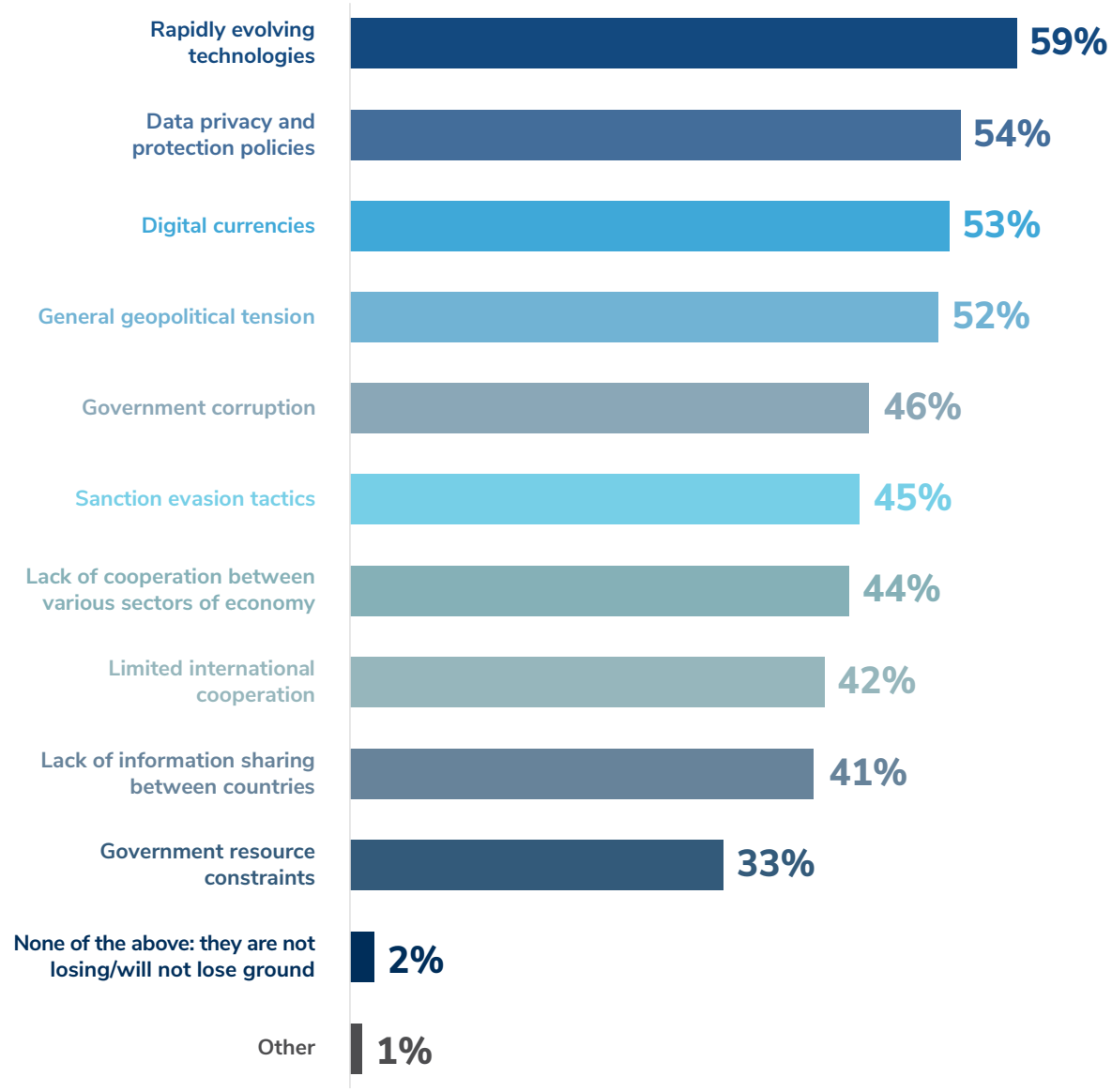
Globally, More Than 60% Expect an Uptick in Enforcement Action and Transparency Levels as it Relates to Sanctions Compliance



In the UK, the Economic Crime and Corporate Transparency Bill has introduced enhanced data sharing measures, which facilitate data sharing among the registrar, law enforcement, government bodies and the private sector. Future changes to the Data Protection Act (DPA) may also allow for information sharing between specific agencies or for specific purposes (for example, the prevention, detection and investigation of financial crime). However, to allow for data to be shared safely and effectively among all these parties, legal provisions must be complemented by the use of technology.

Other significant challenges governments face are rapidly evolving technologies, the increasing use of digital currencies and geopolitical tensions. All these challenges, including data privacy were cited by most respondents as the emerging reasons why governments are losing or might lose ground in the fight against financial crime.

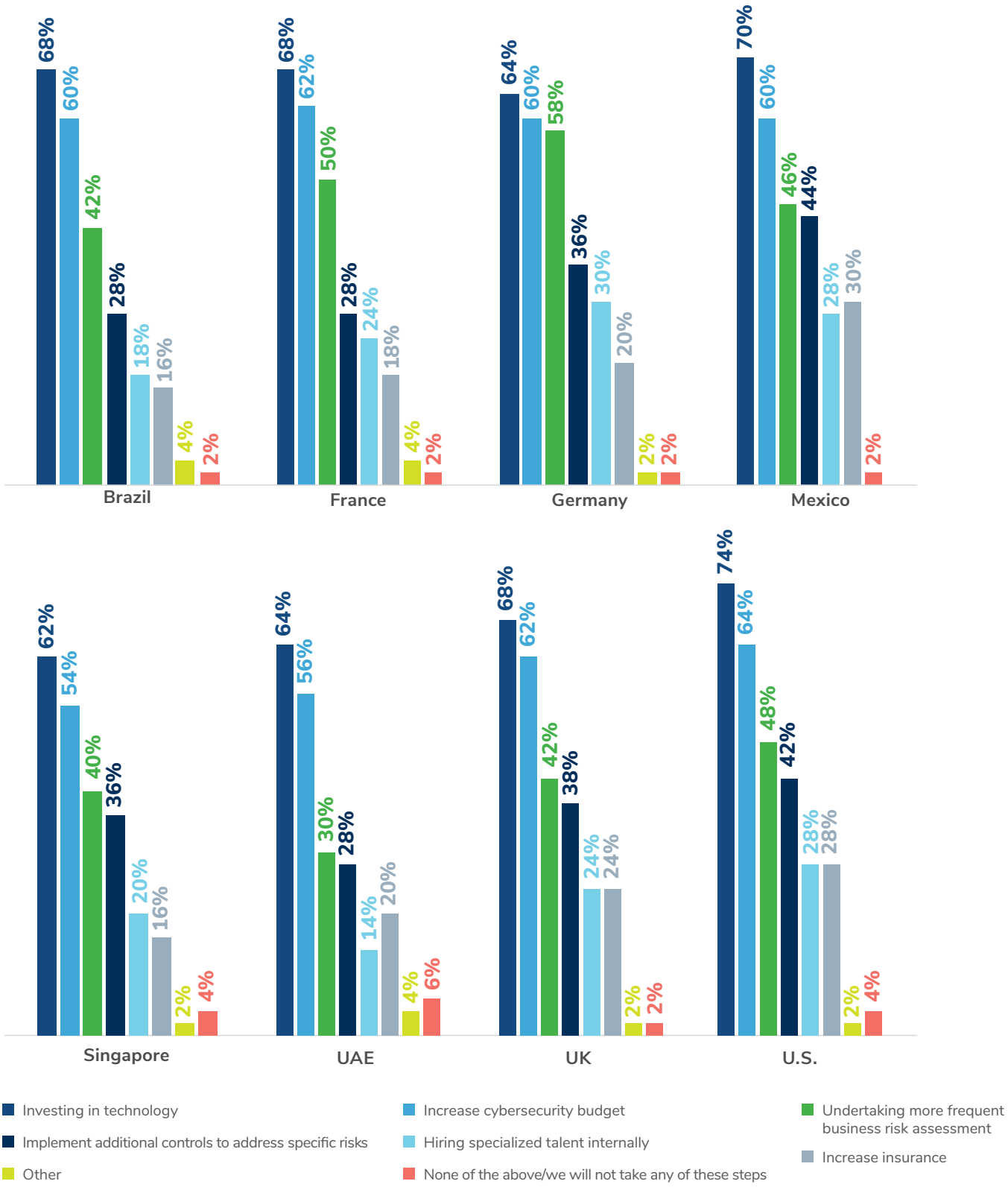
What are the Top Challenges Governments Face in the Fight Against Financial Crime?



The Cost of Compliance and Other Technology Drivers

The increase in financial crime exacerbated by world events and the threat represented by the changes introduced to the legislation and by regulators becoming more active in issuing large fines, have contributed to the growth of the compliance industry. As a result, the compliance costs firms must face to fight financial crime is skyrocketing. In the UK alone, the cost of compliance has exceeded GBP 30 billion, which, according to the National Crime Agency (NCA), corresponds to approximately three-quarters of the government's annual defense expenditure. Despite the increasing costs, as mentioned earlier, FIs struggle to comply with new and existing regulations.

The Majority Plan to Invest in Technology and Increase Cybersecurity Budget to Address Financial Crime Risks



The existing pressure on firms to reduce costs, the demand for technology and the innovation experienced in this sector have led to the rapidly growing use of technology to identify and fight money laundering. Technology investment, increase in cybersecurity budgets and undertaking more frequent business risk assessments have been cited by respondents as the three main steps that firms intend to take during the course of the next year to combat the increase in financial crime.

Regulators and standards setters, such as the Financial Action Task Force (FATF), have also started showing a favorable attitude towards the use of technology. Increasingly, regulators use innovative technology to support supervision and examination ("Suptech") and encourage the use of new technologies by firms to comply with regulatory requirements more efficiently and effectively ("Regtech"). Further, firms can integrate RegTech with compliance software such as Resolver to further engage control owners and conduct regular compliance risk assessments.

In the U.S., the Anti-Money Laundering Act (AMLA) of 2020 supports the use of innovative approaches such as machine learning to reinforce FIs' and Financial Crimes Enforcement Network's (FinCEN) crime detection capabilities. The AMLA also contains provisions for the creation of a Subcommittee on Innovation and Technology composed of innovation officers to advise on means to support technological innovation.

In Singapore, the Monetary Authority of Singapore successfully introduced a new digital platform named Collaborative Sharing of Money Laundering and Terrorist Financing Information & Cases (COSMIC) to share information on customers and transactions between FIs which should, in the long term, address a common challenge that most FIs globally face.

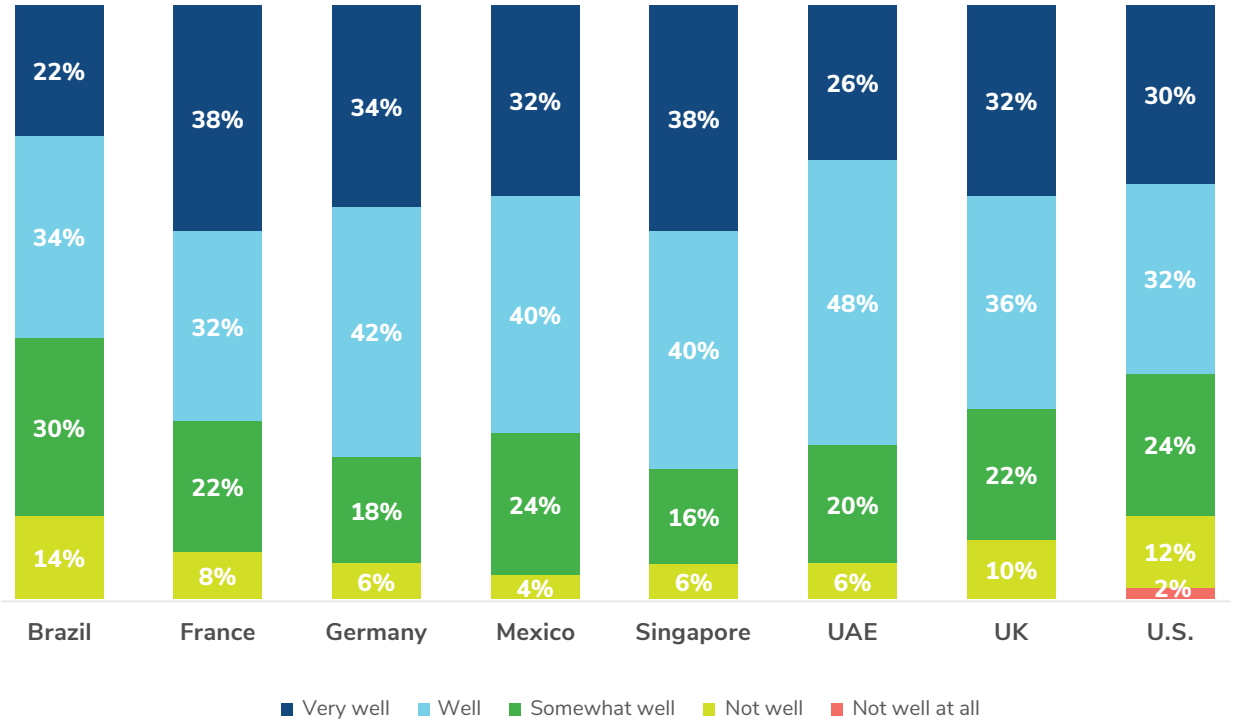
Many speculate that regulatory visits will start looking more closely at the use of technology as part of firms' AML compliance programs.

Carefully Choose Your Technology Solution

Technology can be transformative, improve both efficiency and effectiveness and reduce the cost of compliance in the long term. However, to choose the most appropriate technology solution among the significant number of alternatives available, firms must understand what their objectives are, what each solution can offer as well as its limitations and how this can help the firm achieve those objectives. Key areas firms should consider are the nature, scale and complexity of their business, maturity of their compliance programs and the age of their operating environment and technological solutions.

There are a number of reasons why one should invest in technology. For example, replacing an old customer relationship management (CRM) system and integrating it into cutting-edge monitoring tools can allow better detection of unusual activity, high-risk customers and other risk events. Integrated systems can also allow speedy management information (MI) reporting, reducing the time employees spend on the preparation of reports. Often, firms use old operating systems that do not allow new technological solutions to even be implemented.

How Well do Organizations Understand Their Company's Financial Crime Risks?



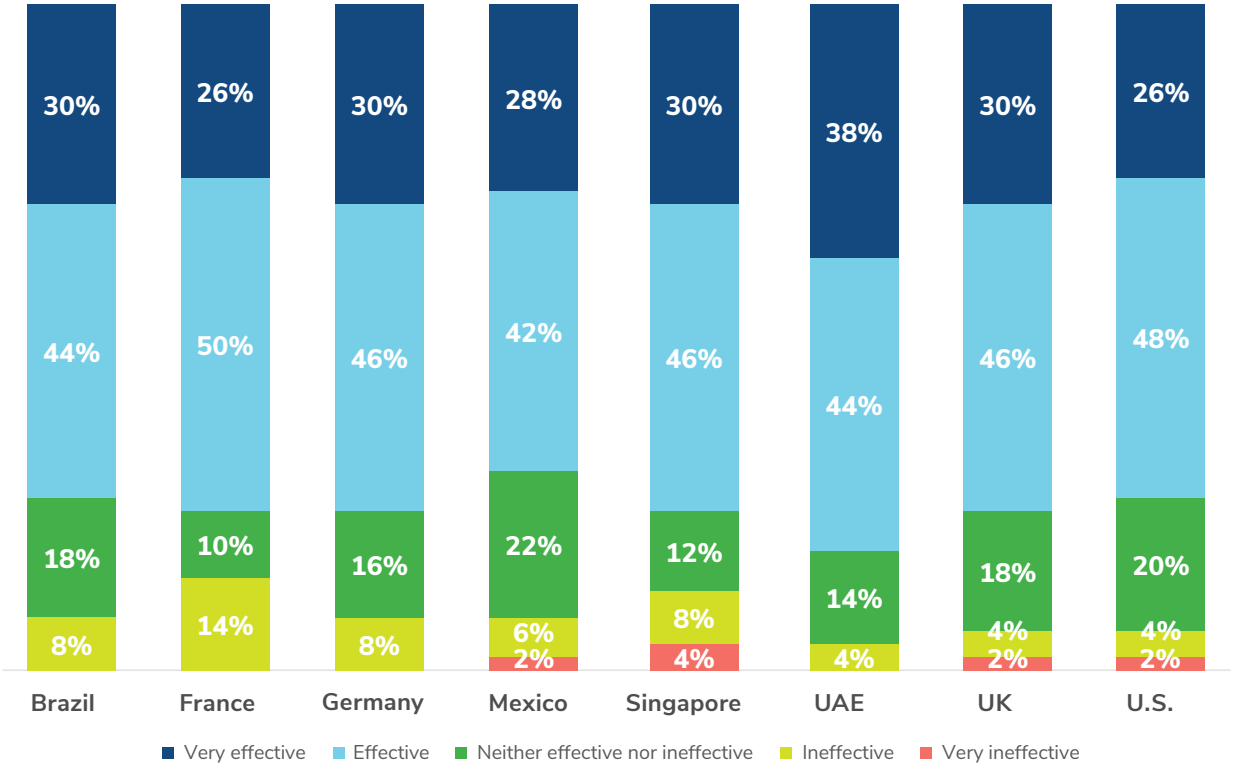
Depending on the specific goals firms have set for themselves, whether these consist of detecting or preventing financial crime, or simply reducing their costs of compliance, firms need to identify and understand the drivers behind their business and adopt a risk-based approach to AML, counter-terrorist financing (CTF), counter-proliferation financing (CPF) and sanctions. Business risk assessment processes would help to identify whether existing systems are not fit for purpose—one technology solution may not be the most appropriate for all the firm's business lines. Hence, consideration should be given to whether multiple solutions should be deployed. For firms to be able to extract as much value as possible from the technology solution adopted, its use must be tailored to the business' specific exposure to those risks. Somewhat surprisingly, 70% of our respondents globally indicated that they have a good understanding of their risks.

This result is consistent with respondents also indicating that conducting more frequent business risk assessments is one of the necessary steps to combat the increase in financial crime.

In addition, somewhat consistently with this data, the percentage of firms from the EU, the UK, Singapore and the U.S. who think their compliance program is very effective only ranges between 25% and 30% while the percentage who think that their compliance program is effective ranges between 45% and 50%.

Can Technology Replace People?

Companies Rate the Effectiveness of Their Financial Crime Compliance Program



There is an argument that the efficiencies introduced by technology will result in unemployment. We believe this is a misconception. The real benefit of technology often resides in increasing people's value by allowing them to manage their time more efficiently and focusing on more valuable tasks, where they can use their expertise and judgement.

Although it can be argued that certain technology solutions can, in fact, replace individuals, the biggest potential advantage is that they can free up people to focus on what they do best, maximizing the value of human expertise and judgement. For example, where the use of technology allows systems to produce a smaller number of false positive alerts, teams can complete their investigations on the alerts faster, report suspicious activity reports (SAR) in shorter timeframes and provide more accurate information to the authorities, contributing to more focused financial crime prevention. Equally, the employee's time can be spent on other projects which would benefit the strengthening of the financial crime framework.

Technology is Not a Panacea

Technology is unable to cure a firm's existing internal weaknesses. Where a firm's internal processes are generating no results or incorrect results, the use of technology may only enhance its existing shortcomings. If internal processes are generating no results or incorrect results, then the initial technology adoption should be one that supports the development of and adherence to effective policy. From there, additional technologies can be layered on. Thus, it is important to consider the flexibility and growth potential of a software platform when making decisions around technology investments.

Integration or application programming interfaces (APIs) between various software and Software-as-a-Service (SaaS) programs can be a cost-effective and time-saving solution if properly executed; however, their application has yet to be attempted by most firms.

Although software providers do offer integrations, (for example, know your customer (KYC) and transaction monitoring systems), these are in practice rarely adopted across multiple internal and external systems. Most compliance programs still feature employees using a number of internal and external systems simultaneously, which may affect efficiency and be prone to mistakes.

Initiatives such as Transaction Monitoring Netherlands (TMNL) and COSMIC are valuable examples of initiatives featuring collaboration among multiple banks. Pooling resources and using advanced algorithms and machine learning (ML) technologies allow organizations to detect patterns and anomalies in transaction data or share with one another information on customers that exhibit multiple red flags. This enables organizations to monitor and analyze transactions across different banks and FIs and spot potential illicit activities.

Data quality underpins AI and ML. Low quality data, including inaccurate or out-of-date data, can negate the benefits of data pooling and collaborative analytics, resulting in erroneous analytical outcomes, preventing the proper functioning of the technology itself and, therefore, hindering its effectiveness.

Kroll's experience in conducting large money laundering remediation projects revealed that the data stored by firms is often inaccurate as it constitutes the outcome of improper KYC and ongoing monitoring historically conducted on customers and transactions. Despite the number of fines issued by regulators, firms persist in investing in technology solutions without prior remediation of the existing data.

If investing in a specific technology solution is not an option, significant results can still be achieved by using a small team of technology experts. Kroll's experience in the biggest and most complex money laundering investigations and remediations revealed that a few technology experts—who know how to analyze data and how internal systems operate—can help firms achieve significant results by spotting patterns and trends and identifying loopholes, hence, understanding what does and does not work.

Before making a large-scale investment in a particular technology solution and embarking on a large transformation project, firms should test the solution as part of ring-fenced practical exercises using a group of specialists solely focused on achieving a specific goal.

By investing upfront in systems, controls, technology and people, firms can protect themselves against the risk of facilitating money laundering and avoid facing the significantly higher cost of remediating their failings. In the long term, this will translate into major cost savings and will contribute to economic growth and to the fight against financial crime and corruption.

References:

https://www.thedigitaleconomist.com/_files/ugd/92dfa2_04fbfaa35ab140ecb62d166bffeec896.pdf

https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html

https://www.fatf-gafi.org/en/publications/Digitaltransformation/Data-pooling-collaborative-analytics-data-protection.html

Optimize Customer Onboarding to Fight Financial Crime

by Ned Kulakowski and Holly Noonan

Customer onboarding can be overshadowed by other aspects of an organization's compliance program, often viewed as a "check-the-box exercise" that doesn't necessarily make the headlines. However, customer onboarding is not only a foundation to any sound program as the first line of defense against risk but also is a cornerstone of compliance. Information obtained during onboarding is not static, but dynamic, used to better understand a customer's purpose and relationship and to help mitigate financial crime risks. This data can inform the entire customer lifecycle, including risk assessments, identification of beneficial owners, periodic reviews, politically exposed person (PEP) and sanctions screening, transaction monitoring and fraud prevention.

This information can be used to mitigate risks or even detect unusual behavior, especially in light of how improper or incomplete beneficial ownership information can be used to obscure corporate structures. Additionally, obtaining beneficial ownership is crucial to being compliant with sanctions concerns, ensuring that sanctioned companies or individuals do not lie within a complex ownership structure or utilize a shell company to launder money.

Information Cannot Exist in a Vacuum

Customer identification and documentation obtained at the onboarding stage is an integral first step to protecting against financial crime risks. A know your customer (KYC) program is a best practice for most companies and a requirement for financial institutions (FIs). This begins at customer onboarding and requires FIs to collect appropriate information and verify their customers through obtaining the correct information as required. In addition to obtaining personal information to verify their customers, FIs should conduct customer due diligence (CDD) to obtain additional information on the customer. This is important to not only be compliant with financial regulations but also protect FIs against financial crime risks.

The information collected during this process is essential to knowing the customer, understanding the expected transactional activity and identifying any jurisdictional risks. Collecting appropriate information is also crucial in providing an accurate risk rating and ensuring that the correct level of due diligence is conducted on higher-risk customers. The information is the first step to knowing who your customer is and to identify any red flags in the transactional activity or customer documentation.

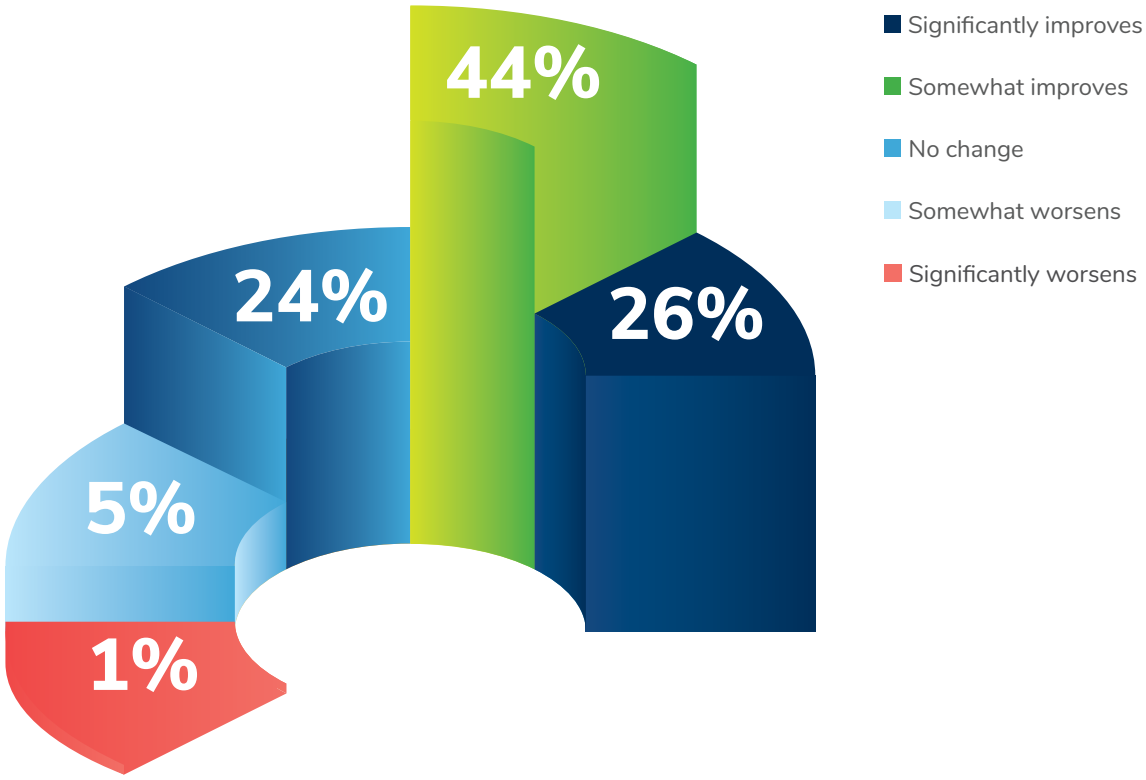
This information continues to be useful for the second line of defense. Investigations into customer activity, such as a review of transactional activity, may use CDD information such as an individual's occupation or a business' profile to determine if the activity is unusual. Additionally, expected transactional activity entered at onboarding can help the second line of defense address issues should there be sudden changes in the amount and type of activity.

Since customer onboarding is an important step to ensuring institutions know their customers, help institutions identify any suspect activity and protect FIs from financial crime risks, it is imperative for institutions to have a robust and efficient onboarding process.

Remote Onboarding: The New Normal

The COVID-19 pandemic likely contributed to the rapid increase in the use of remote onboarding. Our survey results certainly indicate that remote onboarding has a favorable view in the industry, especially in highly regulated industries. Despite this overwhelmingly positive view, the chances of bad actors exploiting the institution by engaging in illicit activity increases, especially if there are faults in the technology, or if those using it on the compliance side of the organization are not trained appropriately. As much as remote onboarding can help move business along, there remains the human element of reviewing this data and making determinations about its accuracy and risk. As stated earlier, a well-implemented onboarding process is a way to address these concerns and is the best first line of defense.

Seventy Percent Say That Remote Onboarding Improves Timing and Efficiency

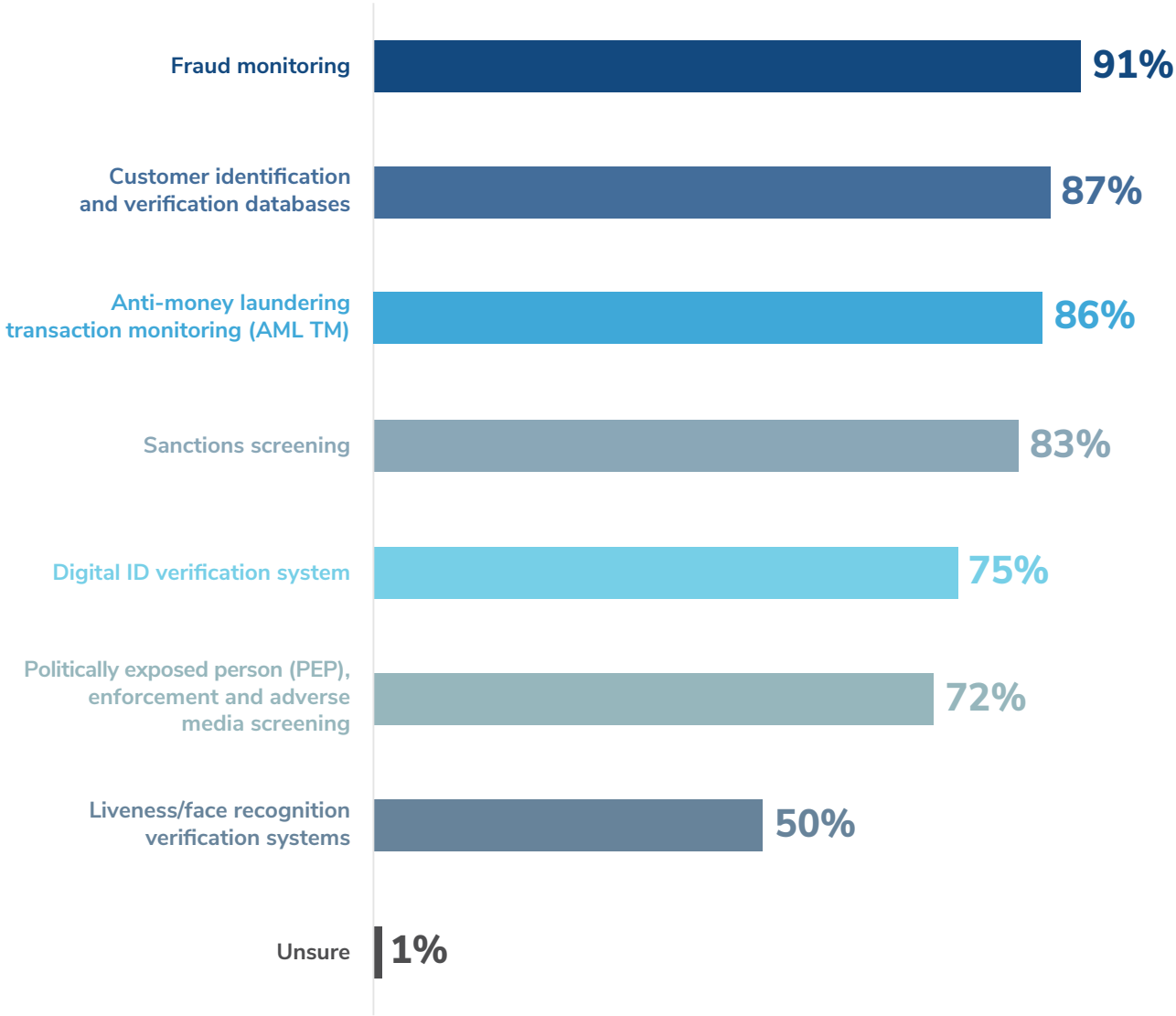


Onboarding information can be used throughout the client life cycle. However, if the data is inaccurate, out of date or missing, this wave of bad data flows through subsequent ongoing monitoring processes, making it less reliable for other users.

Another notable aspect of the survey was that 6% of survey takers stated that remote onboarding either "somewhat" or "significantly" worsened timing and efficiency of customer onboarding. Although outliers compared to others surveyed in their jurisdictions, it is intriguing that some countries would express a concern about efficiency. Is it due to being in highly regulated regimes? Or is it because their own companies require more onerous procedures when remote onboarding is involved?

Overall, our survey results indicate that highly regulated industries have embraced remote onboarding technology with 70% of global respondents confirming it improves the timing and efficiency of the process. Technology and its use are clearly being encouraged by regulators, governments and industry bodies. But how does this affect the onboarding and monitoring aspect of a compliance program? Remote onboarding, which does not require any form of in-person verification, is open to many opportunities for fraud. Because of this, remote onboarding may trigger additional verification and monitoring steps, which fall on the institution to absorb.

Which of the Following Financial Crime Tools are Most Commonly Used?



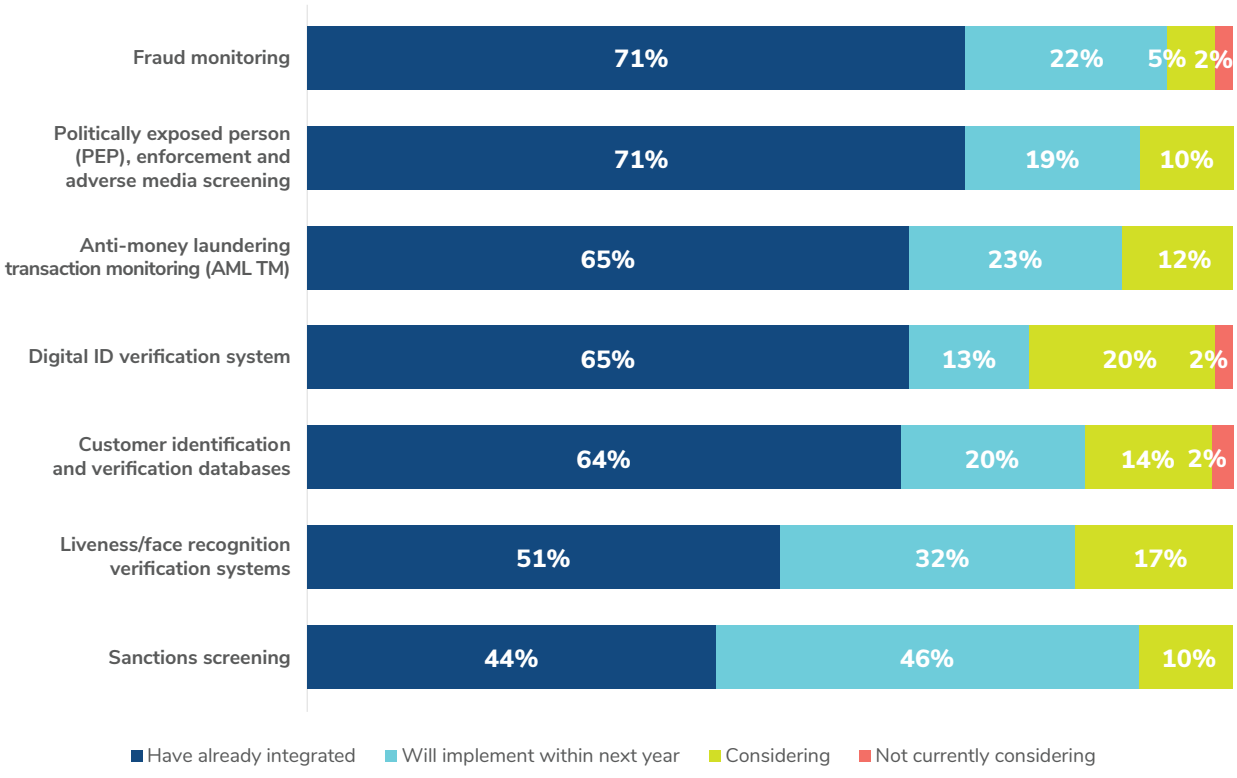
Interestingly, most of those individuals surveyed by Kroll utilize a host of compliance tools, including 91% using fraud monitoring, 87% using customer identification and verification databases and 86% using AML transaction monitoring. Even the lowest response within the survey was 50%, where survey respondents indicated they are currently using liveness/facial recognition systems. Half of the respondents saying they utilize facial recognition technology is surprising as this technology is continually evolving and relatively new compared to other data tools. Additionally, none of those taking the survey stated that they do not use any of these tools. This is not surprising due to the amount and breadth of technology admittedly used, at least among the larger regulated industries that were surveyed.

However, if these systems are used in a vacuum, not only in terms of the systems themselves but also between different compliance departments, it brings into question whether they are being used in the most effective manner. Is integrating them a solution?

Integration as the Future

It is an all-too-familiar scene across every industry: the employee who has five different systems open on their computer screen (or multiple computer screens) at the same time, trying to use, review and reconcile all data while performing their work duties. The employee then has to save the information to a specific location for audit and regulatory purposes. Issues may still arise if they don't have access to a particular software program or database and cannot get the information themselves. They may have to go to another employee, which then opens additional issues regarding access, privacy concerns and the sheer organizational red tape that may be present.

Which of the Following Financial Crime Tools are Most Commonly Integrated?



As seen in the survey, internal integration of surveillance tools has either occurred or will occur within the next year, according to the majority of the survey takers, including 93% for fraud monitoring and 90% for PEP, enforcement and adverse media screening. Integration between internal systems at an institution would seemingly be a positive development in terms of work efficiency and in data quality and accuracy. Certain internal data sources may have more data than others and may also contain more detailed or even conflicting information that warrants additional review. However, does integration aid in the ongoing fight against financial crime? Is this a reflection of regulatory pressure or pure innovation on the part of these surveyed institutions?

Internal systems alone can provide a wealth of data and should be used across the organization to help address financial crime and fraud issues. However, as good as integration is, a human reviewer, trained to use and to interpret how the information fits together, will be needed. Application programming interfaces (APIs) between internal systems can greatly increase efficiency and accuracy of data. Should this also be considered in terms of interfacing between external systems, SaaS products and government systems?

In the area of KYC and CDD, an item becoming more frequently discussed is the concept of "perpetual KYC" or "dynamic KYC." When compared to the more traditional approach, perpetual or dynamic KYC information is continually refreshed, reviewed, interpreted and integrated into other systems based on information obtained throughout the client's lifecycle, whether it be from transaction monitoring or other screening sources. It is not static data that is refreshed manually every few years, as has been the case with traditional KYC. This ensures more accurate information is on file, which then trickles down to the other lines of defense.

The concept of data integration works between other systems as well. An example would be KYC information being used to assist in the sanctions screening, transaction monitoring and fraud detection processes. Sanctions alerts could trigger a review of customer's transactions and vice versa. However, none of these integrations are helpful if the individuals reviewing the data don't understand what they're looking at or how to interpret the data.

Overall, systems integration can be a key component to a financial crime compliance program, but it is only as good as the data itself, as well as the people who are using it. It comes down to communication between different lines of an organization, breaking down groups that are siloed and training compliance and business lines so that each knows what the other is doing. In the long run, this organizational direction will greatly help in the fight against financial crime.

Beneficial Ownership and Corporate Transparency in Flux

by David Lewis, Ned Kulakowski and Maria Evstropova

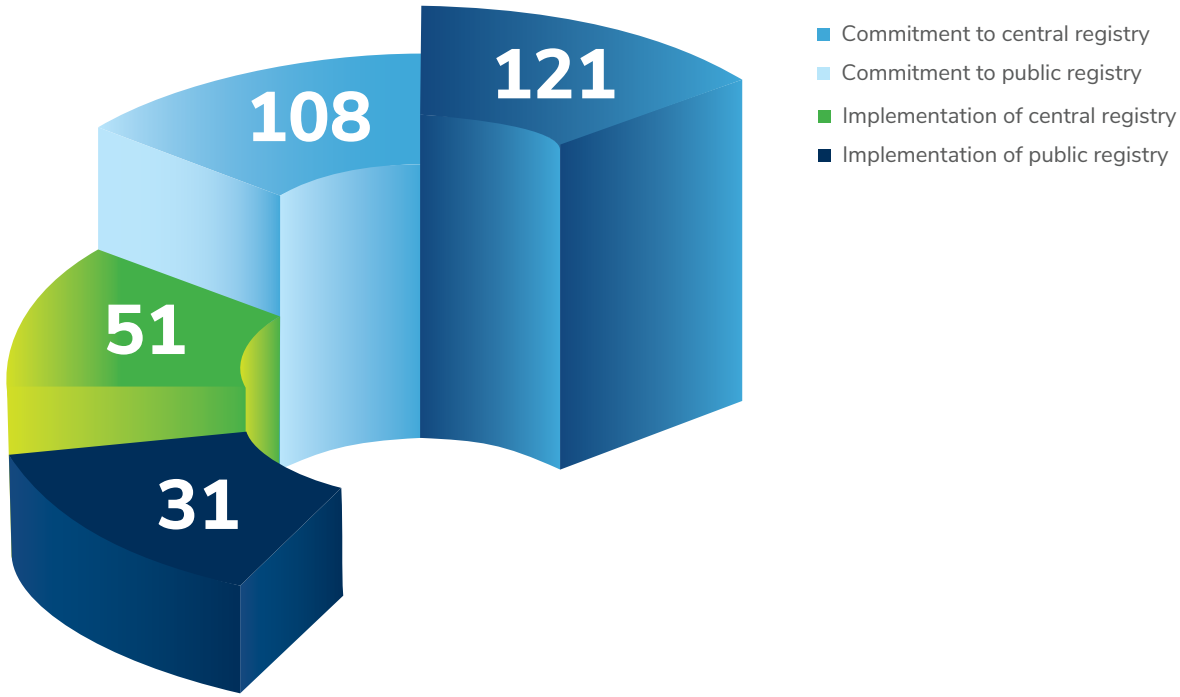
Financial crime comes in all shapes and forms, from drug cartels laundering profits through legitimate businesses, to the rich and powerful offshoring their wealth, to students used as money mules buying million-dollar properties for unknown individuals. One common element that makes these crimes go undetected is the frequent use of shell companies. With their often-bogus officers and opaque corporate ownership structures, these companies disguise the true identities of those behind it.

Corporate transparency has been a subject of interest for several decades and it continues to be at the heart of discussions about financial crime, breaches of sanctions, tax evasion and secrecy concerns. Having access to a central beneficial ownership registry with accurate, up-to-date information where corporate entities declare which individuals control them would be instrumental in the fight against financial crime and could close a major loophole that has routinely been taken advantage of by various corporate and individual actors.

According to our survey, there is little question among financial institutions (FIs) and corporate entities about the utility of a beneficial ownership registry; 87% of respondents globally stated that a beneficial ownership registry would be "somewhat" or "extremely helpful." Although routinely thought of as an onboarding information source, complete and accurate beneficial ownership information can be leveraged across multiple business lines throughout the customer relationship and can be used in numerous ways to address risk. There does, however, appear to be some uncertainty about which jurisdictions around the globe are participating, according to our survey. Other questions remain around central registries, including who will be able to access the information, who will have to register to see the information and how much information will be included in each entry. As stated in the "*How Technology is Transforming AML*" article, technology can be vastly helpful in this space. In the case of beneficial ownership registries, having direct access and integration with systems, along with coordination between public agencies and the private sector, can be extremely useful to compliance departments. However, a beneficial ownership registry is not a panacea. No matter the level of accessibility or the quality of the data, institutions will still be required to perform their own research and diligence on parties; a beneficial ownership registry remains merely a tool in the arsenal used by compliance professionals in the fight against financial crime.

Who Has a Registry, and Who Has Committed to One?

Beneficial Ownership Registries Worldwide



Source: Openownership.org

The idea of public beneficial ownership registry dates back to the 1990s, but it wasn't until the early 2000s that the concept gained traction among policymakers. In 2003, the Financial Action Task Force (FATF), an intergovernmental organization that sets global standards for combating money laundering and terrorist financing, published a recommendation that countries should require all legal entities to maintain beneficial ownership information and make them available to law enforcement and competent authorities. In 2009, the G20 endorsed the FATF's recommendation and called on all countries to adopt measures to prevent misuse of legal entities for illicit purposes. In 2012, the FATF strengthened its standards on beneficial ownership and issued additional guidance on transparency and beneficial ownership in 2014, further clarifying what ownership and ultimate effective control mean.

The first country to establish a public beneficial ownership registry was the UK, launched in June 2016. This was followed by similar initiatives in other countries, including Ukraine, Colombia, Kenya and Nigeria, who now maintain public beneficial ownership registries.

In 2018, the EU adopted the 5th Anti Money Laundering Directive (5AMLD) requiring all EU member states to establish central registries containing information on the beneficial owners of legal entities, including trusts established within their jurisdiction by March 10, 2020. However, in November 2022, the European Court of Justice ruled that the general public's access to beneficial ownership information meant "serious interference with the fundamental rights" of both private life and personal data. As a result of this ruling, some EU members, including Luxembourg and the Netherlands, suspended access to their registers to the public and have since introduced additional rules on who can access registry information.

In the U.S., the Corporate Transparency Act (CTA), as part of the Anti-Money Laundering Act (AMLA) of 2020, contains a beneficial ownership information reporting requirement, effective January 2024, for certain corporations, limited liability companies and other entities. Entities will be required to file a report with the Financial Crimes Enforcement Network (FinCEN), which identifies an entity's beneficial owner and provides information about the persons who formed the entity. However, many details about this registry remain uncertain, including to what extent outside groups, such as FIs, will have access to this information.

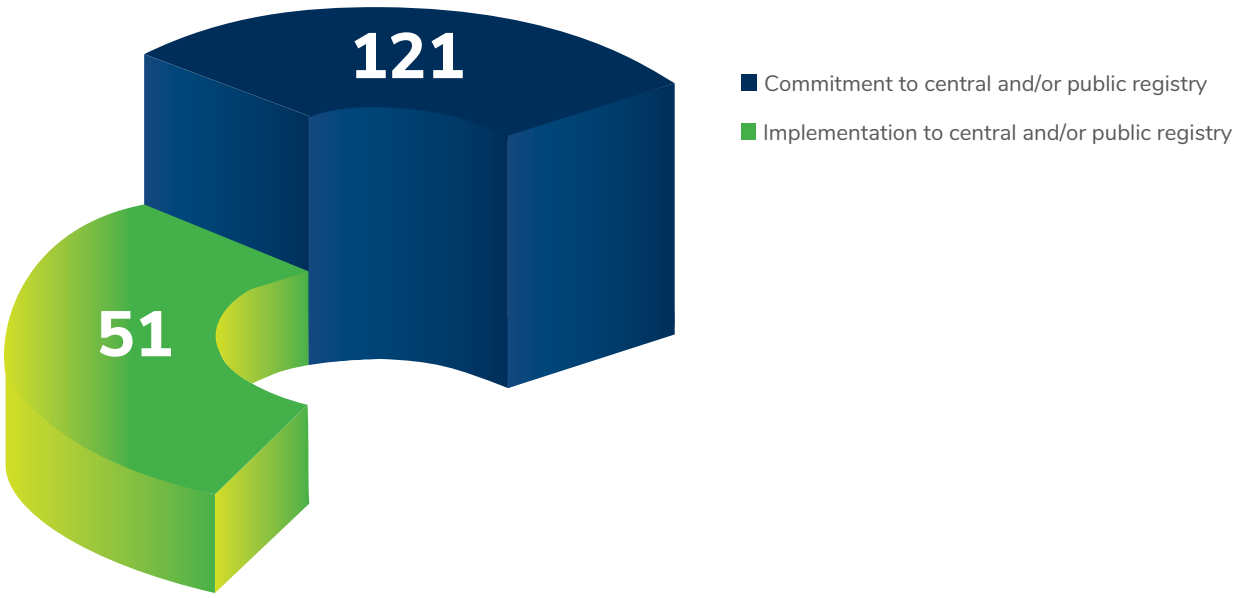
Canada announced in March 2023 that it will implement a free and publicly accessible beneficial ownership registry of all corporations, a big step in a jurisdiction that has frequently come under criticism for its money laundering issues.

Some countries have put legislative provisions in place requiring mandatory submission of beneficial ownership information and commitment to establishing a registry. However, not all of them are, or will be, publicly accessible. India is an example where companies are required to disclose the details of beneficial owners, directors and key personnel to the government, but access to the register is not public.

More countries are establishing, or committing to establishing, a dedicated beneficial ownership registry, and although the access to the information may be made available to the public in some instances, beneficial ownership information is not readily available in most jurisdictions due to inadequate regulation or poor enforcement of laws.

The information may also vary across jurisdictions due to the myriad of definitions of ultimate control, along with varying reporting thresholds and reporting requirements. Furthermore, data privacy concerns and compliance and professional risks, to name a few obstacles, make effective implementation of reporting standards even more challenging.

Commitment and Implementation of Beneficial Ownership Registries Worldwide



Source: Openownership.org

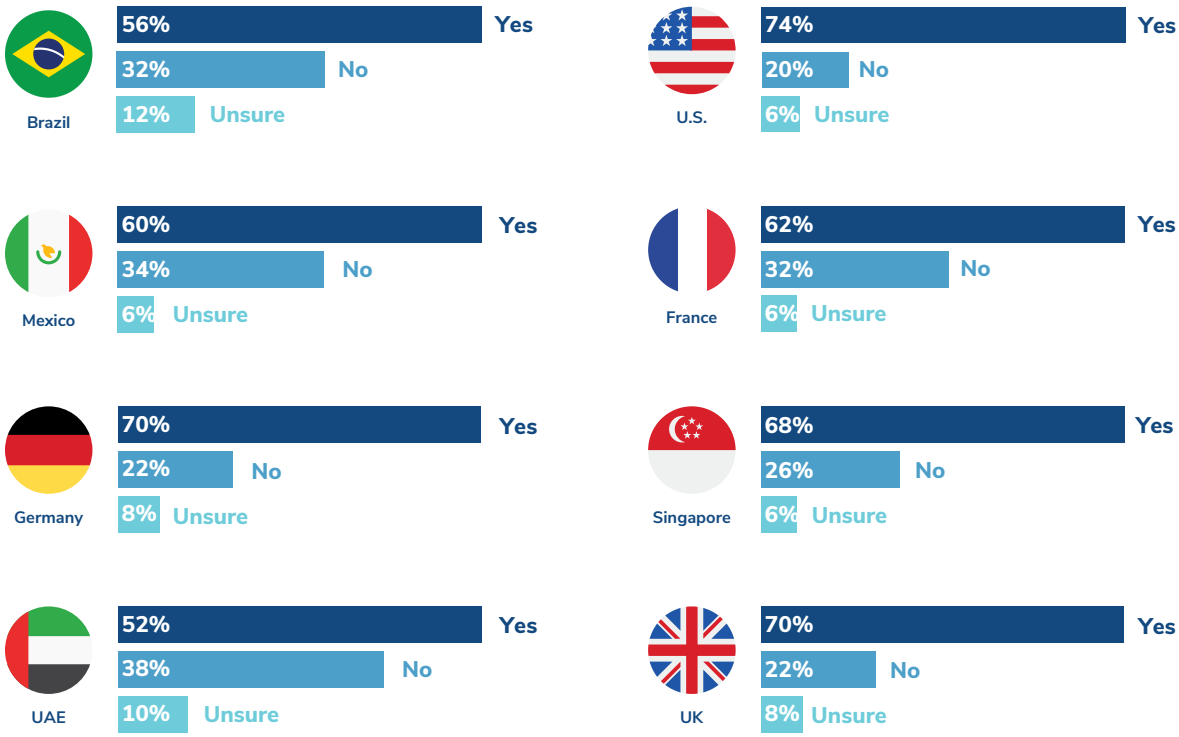
An Evolving Story: What Does "Access" Truly Mean?

Nearly two-thirds of those who took our survey stated that they have access to, or anticipate having access to, their jurisdiction's beneficial ownership registry. Another 28% state that they do not currently have access to, or do not anticipate having access to, a registry. A small 8% of survey respondents were unsure. The two-thirds majority brings into question how informed practitioners stand on this issue around the globe. It is likely that many of those individuals who answered "yes" would fall into the category of anticipating registry access. As indicated above, many jurisdictions have not yet established a registry, and the question remains: once these registries are rolled out, who will have access and to what degree? For example, in the U.S., debate swirls around the level of access bank employees will have, as opposed to those in law enforcement or in the government. The way the current proposed rule stands, outside entities such as banks will have very limited access.

Does the survey suggest that the 28% who said "no" are correct? Is this a question of misinformation or a lack of understanding by those out in the field? This suggests that there is a need for better education explaining and clarifying to those in the industry who will have access, and what information will be contained within each registry.

Overall, the current situation is evolving globally and is in constant flux. It will require vigilance on the part of everyone to keep on top of these changing requirements and adjust their programs accordingly.

Over Two-Thirds Have Access or Anticipate Having Access to Their Jurisdiction's Beneficial Ownership Registry

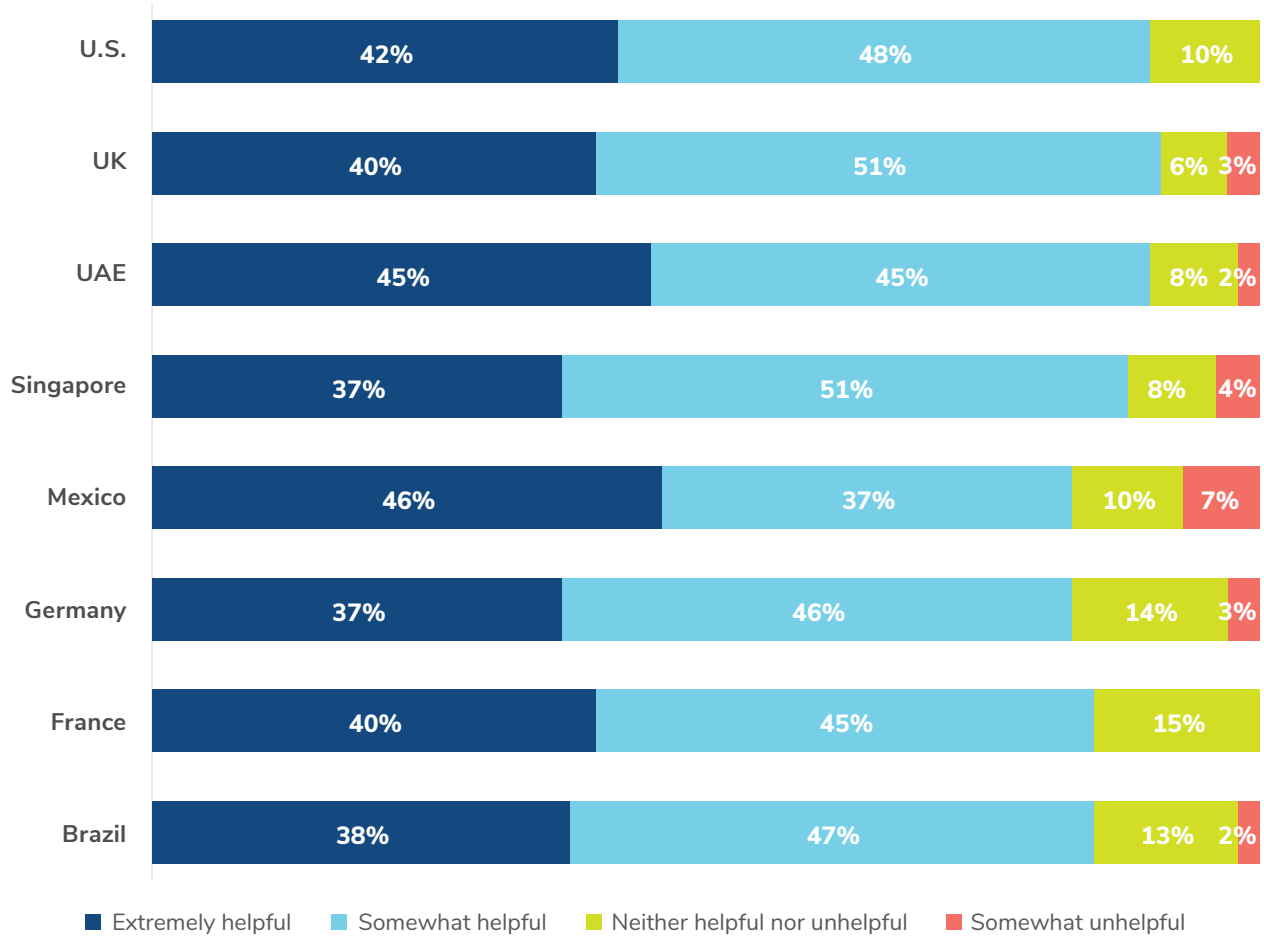


Helpful, But How Much?

The consensus among survey takers who have access to their beneficial ownership registry is that it will be either somewhat or extremely helpful to their compliance programs. Very few believe access would be unhelpful, clearly indicating that, regardless of whether full or even partial access ever becomes fully realized, there is an overall agreement that access would play a key part in one's compliance program.

With individuals and corporate entities filing their own information with central registries, the reliability of the data is in question. This can bring a host of issues. For example, the ability to mistakenly check the wrong boxes or have the option to be less than transparent by checking "unknown," as has been proposed in the U.S. Also, there is a debate in the final rule about the AMLA's provision concerning the "consent" requirement that parties who have filed beneficial ownership information need to provide to other parties, such as banks, access to the information.

Beneficial Ownership Registry is Helpful to the Majority of Companies Surveyed



What if the information that is within the corporate registry itself conflicts with other documentation that the entity has submitted? Similarly, what if a bank employee finds inconsistencies in what is in the registry documentation and forms and what they have been provided directly by the customer, or what they even found researching in the public domain? Is it now on the institution to file a discrepancy report with the regulator? If this is the case, there may be additional obligations at play. For example, does the reporter to the regulator have to perform additional research and provide an ample, detailed explanation of the discrepancy and "fill in the gaps"? Once these steps are taken, this will now put additional obligations on

the institution to determine how to address updating the information in their own systems and performing additional investigations, where necessary, and to even consider whether to exit the client relationship.

In the UK, Companies House has maintained a central beneficial ownership for seven years. As of April 2023, there is now an additional obligation on the part of FIs to report discovered "material discrepancies" on an ongoing basis. These reporting requirements don't appear to be especially onerous, as discrepancy reports only need to be filed if there are money laundering or terrorism financing concerns, or if the discrepancy appears to "conceal the details of the customer's business." Although this now means firms will have to implement more controls and processes around discrepancy reporting, it is certainly a positive step in tackling financial crime.

The recent decision by the European Court of Justice on specific access also raises some questions as to the future of access, and whether the information contained in these registries will prove as much use to the institutions seeking to use them.

Despite the doubts addressed above, along with the additional potential burdens on those who wish to use the data, there is little question that a beneficial ownership registry will prove to be useful, especially a central registry available to FIs. If done right, there is little debate as to a beneficial ownership registries' usefulness in the financial crime space. It is a source of information that can assist in onboarding, investigations and due diligence processes, but it cannot be the only source. Staff should not be lulled into a false sense of security by merely relying on information at face value and taking it as "truth"; onboarding teams or compliance will still have to undertake a form of vetting process, checking the public registry against their own data sources and research. They won't be able to merely present to the regulator that information was taken from the registry and that analysis was stopped there, with no other steps taken. A beneficial ownership registry is a tool that can help corroborate research and data but is not a "magic" solution to the challenges of financial crime compliance.

When asked specifically about how access to a beneficial ownership registry would support their financial crime compliance program, responses ranged considerably. However, a significant portion indicated that it would improve security and could deter financial crime. Notably, some stated that they were either currently evaluating, didn't know, or were unsure how a registry would support their program. When compared to another survey question, which shows an overwhelming belief that access to a registry would be helpful, these responses show that there is some uncertainty as to how this data can be implemented into a program.

Overall, the survey suggests that there would likely be useful information contained in a beneficial ownership registry, regardless of the jurisdiction, despite remaining questions about reliability and how data access will play out. However, no matter how good the registry, cooperation across organizations, governments, regulators, vendors and fintech companies will fundamentally make it more effective and useful going forward. If all users and consumers of the information can contribute in a community-based format, sharing data and findings across their networks would lead to a far more accurate and effective information source.

A central beneficial ownership registry is a fundamental tool in obtaining corporate transparency and in the fight against financial crime. However, questions surrounding accessibility and data quality of beneficial ownership registries continue to raise concerns as to whether the jurisdictions who have committed to such a registry will be able to have one fully implemented. Even if they do, a central registry's overall ability to serve as an asset and not a burden to financial crime compliance programs remains largely unsettled.

Unraveling the Global Impact of Corruption and Bribery

by Michael Watt

Corruption presents a daunting challenge to societies and economies worldwide. It undermines development, destabilizes governments, erodes societal trust and curbs economic growth. Corruption, in its various forms (bribery, embezzlement, nepotism, patronage and graft), permeates many facets of societies globally. Resources intended for public goods and services are siphoned off, leading to substandard infrastructure, including poor quality education and health care systems. In the political realm, corruption undermines public trust, leading to societal instability and conflicts.

Over half of the world's population resides in countries rated as having endemic corruption, which dissuades foreign investment and heightens lending costs. Corruption also acts as a challenge for companies seeking to operate internationally, particularly in remote locations, often beyond the reach of their corporate compliance programs and domestic regulators. With ongoing economic anxiety in the background, the barrier of bribery and corruption demands a more deliberate and effective response from global regulators, banks, corporations and financial gatekeepers.

Direct impacts on banks and multinational corporations are vast, ranging from the financial costs associated with goods and services to reputational damage. Anti-bribery and corruption (ABC) law breaches in most of the surveyed countries have led to substantial civil and criminal liabilities. Many companies representing household brands have paid fines or settlements for contravention of bribery and corruption laws well over USD 500 million.

Given that most survey respondents believe that financial crime is a top challenge for governments, the question remains: What gaps are the private sector expected to fill to address corruption and bribery risks?

Emerging Challenges

Top Challenges Governments Face in the Fight Against Financial Crime

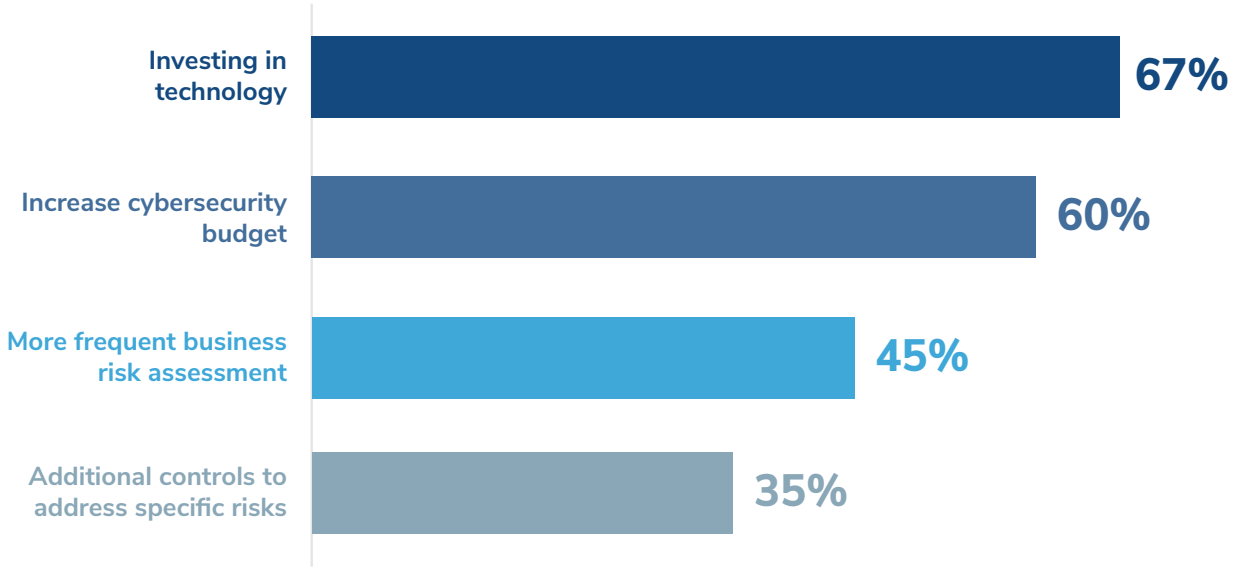
The leading global factors contributing to increased financial crime risks in the next 12 months include cybersecurity and data breaches (33%), financial pressure (16%), the impact of remote work (14%), increased regulatory enforcement (13%) and geopolitical tension (12%). This ranking of factors closely aligns to sentiments found in Kroll's benchmarking surveys of recent years. However, for 2023, increased regulatory enforcement tied for the second-highest rated factor for U.S. respondents (18%).

These factors also align with respondent sentiment of the top reasons why governments are or will lose the fight against financial crime. If organizations believe that governments cannot keep pace with the rapidly evolving technology, how can they be expected to protect the private sector against cyber threats? As cybercriminals advance their tactics, data breaches have increased, exposing sensitive company information. This gap between government and technology can be exploited by financial criminals, either internally or externally, posing significant risks to organizations and their ABC programs.

Whether organizations are most impacted by challenges from technological change, digital currencies, data privacy policies or geopolitical tension, investing in technology, cybersecurity and other preventative measures ensures resilience for ABC programs.

How to Respond

Primary Steps Taken by Organizations to Tackle an Increase in Financial Crimes



Investing in Technology

Investing in advanced technology allows financial institutions (FIs) and multinational corporations to proactively combat financial crime. This includes artificial intelligence (AI) and machine learning (ML) algorithms that analyze vast amounts of data more efficiently and accurately than any human alone could, which helps organizations identify suspicious patterns indicative of fraud, money laundering or other financial crimes.

Blockchain technology, for instance, is increasingly being adopted for its ability to provide a transparent, immutable record of transactions. This technology could be instrumental in deterring and detecting corruption and bribery, thus enhancing the effectiveness of ABC programs.

Increasing Cybersecurity Budgets

Additionally, as financial systems become increasingly digital, the threat of cybercrime correspondingly escalates. Data breaches and cyberattacks not only pose a significant financial risk but also have the potential to cause severe reputational damage. An effective cybersecurity strategy thus forms a critical component of an effective ABC program. Organizations must consider investing in cybersecurity measures like managed detection and response, encrypted communications, effective vulnerability patching and strong authentication protocols. Also, conducting regular cyber risk assessments and implementing comprehensive employee training programs can help detect vulnerabilities, prevent cyberattacks and enhance the overall security posture of the organization.

Integrating AML and ABC Functions

Due to the intertwined nature of financial crime compliance programs detailed throughout Kroll's 2023 *Fraud and Financial Crime Report*, another solution to increased risks and greater cost controls may begin with integrating anti-money laundering (AML) and ABC functions. Many headlines regarding significant bribery and corruption claims include breaches of AML regulation, and vice versa, highlighting opportunity for a collaborative approach within organizations.

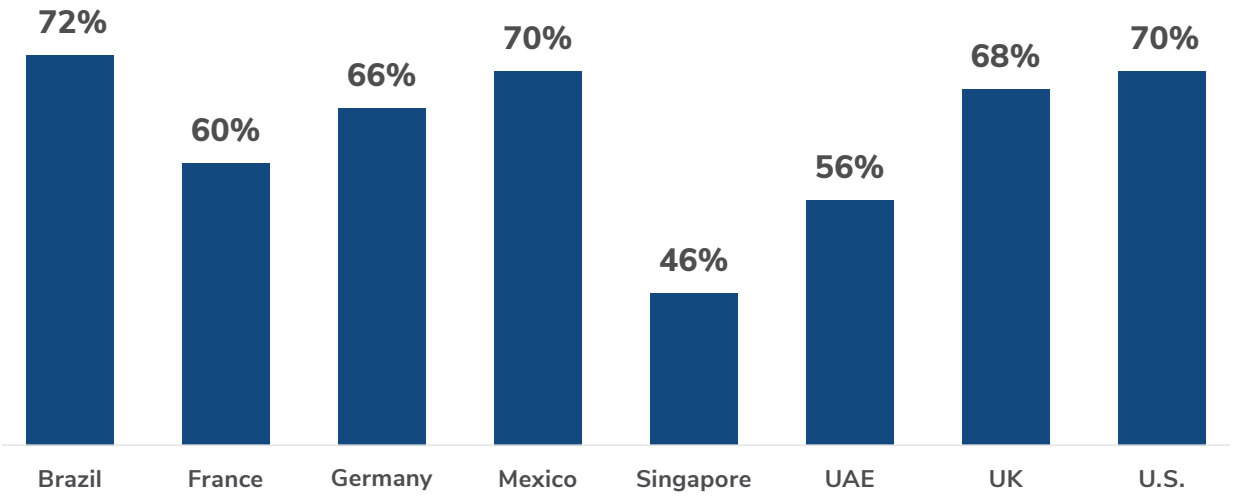
AML and ABC functions are distinct specializations within most financial crime compliance programs; however, they travel in the same direction and utilize similar tools, methodologies and trainings. Efficiencies can be gained when organizations intentionally seek integration by leveraging shared resources for investigations, audits and risk assessments.

Frequent Risk Assessments

Given the dynamic nature of bribery and corruption and its associated risks, regular risk assessments are crucial to ensuring an effective ABC program. These assessments should identify, measure and understand both current and emerging risks, including geopolitical tensions, changes in regulations and technological innovations.

Regular risk assessments allow organizations to stay ahead of the curve, identifying potential vulnerabilities before they can be exploited. Furthermore, they enable organizations to adjust their risk appetite and controls in line with their evolving operating environment, ensuring their compliance program remains fit for purpose and resilient in the face of change. This is why organizations are increasingly investing in integrated risk technologies that unify risk with compliance, cyber and audit to help an ABC program pivot as quickly as world events occur.

Expectations That Enforcement Action Will Increase



Continued Commitment from Governments

ABC programs, in particular, need to stay nimble as the global enforcement environment develops. Globally, the anticipation of increased enforcement actions is on the rise, with over 60% of survey respondents predicting an escalation in the next 12 months.

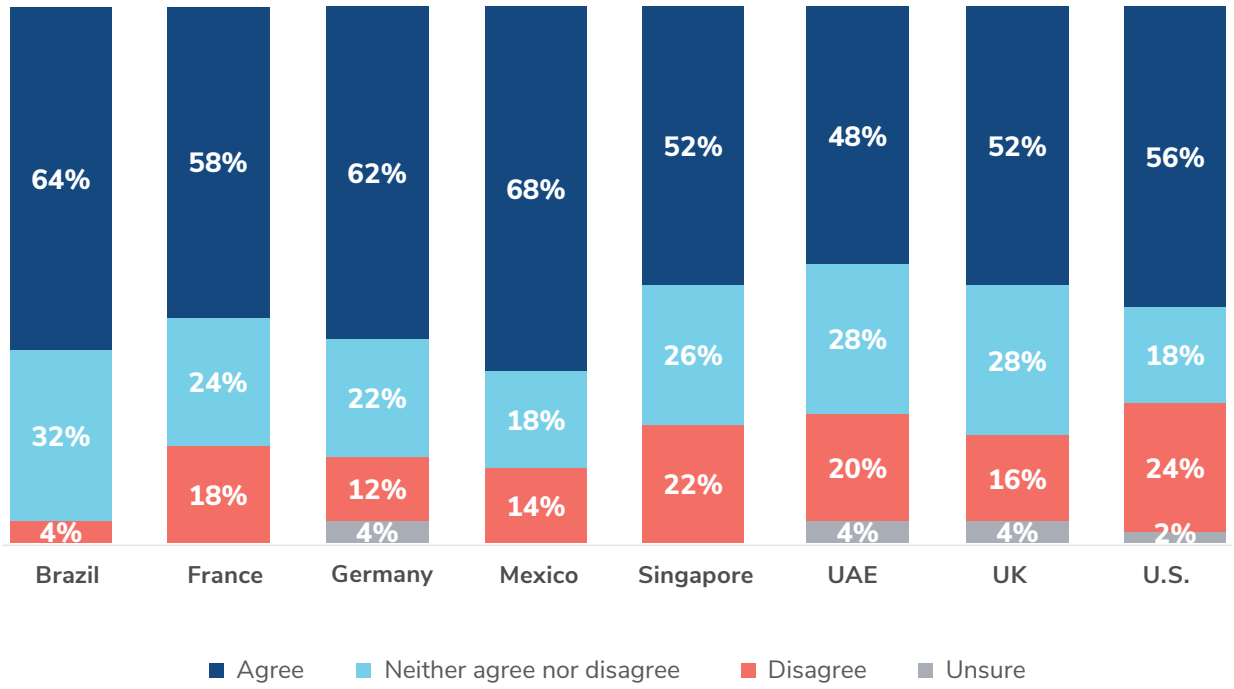
In the U.S., the high expectation of increased enforcement aligns with the continued growth and investment in regulatory enforcement functions. The U.S. Department of Justice (DOJ) has consistently stressed that it views corporate criminal enforcement as a national security issue, which results in an accompanying surge of resources for Foreign Corrupt Practices Act (FCPA) enforcement. While sanctions were dubbed as the "new FCPA" by U.S. Deputy Attorney General Lisa Monaco, the FCPA is still the FCPA and will maintain its prominence in corporate criminal enforcement.

Brazil respondents, always with high expectations for an annual increase in enforcement, demonstrated the highest level of expectation among the surveyed countries at 72%. A new presidential administration may be influencing sentiment; however, new regulations enacted in 2022—Decree No. 11,129/2022—enable administrative and civil liabilities under the Brazilian Clean Companies Act (BCCA). The decree further describes the evaluation parameters for compliance programs that are similar to the U.S. DOJ's 2020 Guidelines on Evaluation of Corporate Compliance Programs. With the maturation of Brazil's anti-corruption law, the effectiveness of compliance programs is expected to follow.

The UAE being a country with a developing regulatory framework and no comprehensive anti-corruption legislation at present, expectations of increased enforcement are relatively high with 56% of respondents. The Penal Code provides provisions for ABC in the private sector; however, ABC compliance programs are not regulated. As is the case with many international business hubs, companies operating in the UAE often follow guidelines from international regulators and their sentiments may reflect the global expectation of increased enforcement. Domestic ABC laws may, nonetheless, be influenced in the coming years by the impact of grey listing from the Financial Action Task Force (FATF). The UAE's progress to be removed from the grey list has drawn attention to a need for improvements to compliance cultures for banks and multinational corporations, which leads to more resilient ABC compliance programs.

A Growing Focus on Gatekeepers?

Agreement Third-Party Gatekeepers Must Help Combat Financial Crime Risk



Looking ahead, regulations on third-party gatekeepers is the next frontier for ABC enforcement frameworks seeking to better combat financial crime, such as in the U.S.

Third-party gatekeepers play pivotal roles in facilitating large financial transactions. Given their positions, they are poised perfectly to detect and prevent corruption. Regulators are moving to take a stricter stance, seeking more accountability, stricter regulations, rigorous oversight and heavier penalties for noncompliance by the gatekeepers themselves.

According to the FATF, of all the countries assessed to date, only five still do not regulate gatekeepers. Out of more than 150 countries, only the U.S., Australia, China, Madagascar and Haiti are yet to regulate gatekeepers. In the U.S., the pending ENABLERS Act, aimed to close loopholes for gatekeepers, continues to be at the mercy of the American legislative process. However, in 2023 or 2024, bipartisan support may be sufficient for the law to be reconsidered. While the majority of global respondents believe that third-party gatekeepers increase financial crime risks, 16% disagree. U.S. respondents have the highest level of disagreement at 24%, which may indicate the proportionate opposition to laws such as the ENABLERS Act.

Looking Forward

As the fight against bribery and corruption evolves, so do the measures used to combat it. Corruption is a pervasive challenge, but our collective efforts can and must rise to meet it. Strong, collaborative measures from governments, regulatory bodies, corporations and individuals globally are critical to curbing its destructive impact.

Despite the considerable challenges, the progress made thus far in combating bribery and corruption offers cause for optimism. We are witnessing a global shift towards increased enforcement, enhanced regulatory frameworks and more sophisticated, technology-driven measures to prevent and detect corruption. By understanding the landscape of economic crime, we can develop proactive strategies to curb corruption, foster ethical conduct and build a more equitable society.

The Future of Sanctions Compliance Programs: Navigating the Challenges of a Complex Global Landscape

by Michael Watt

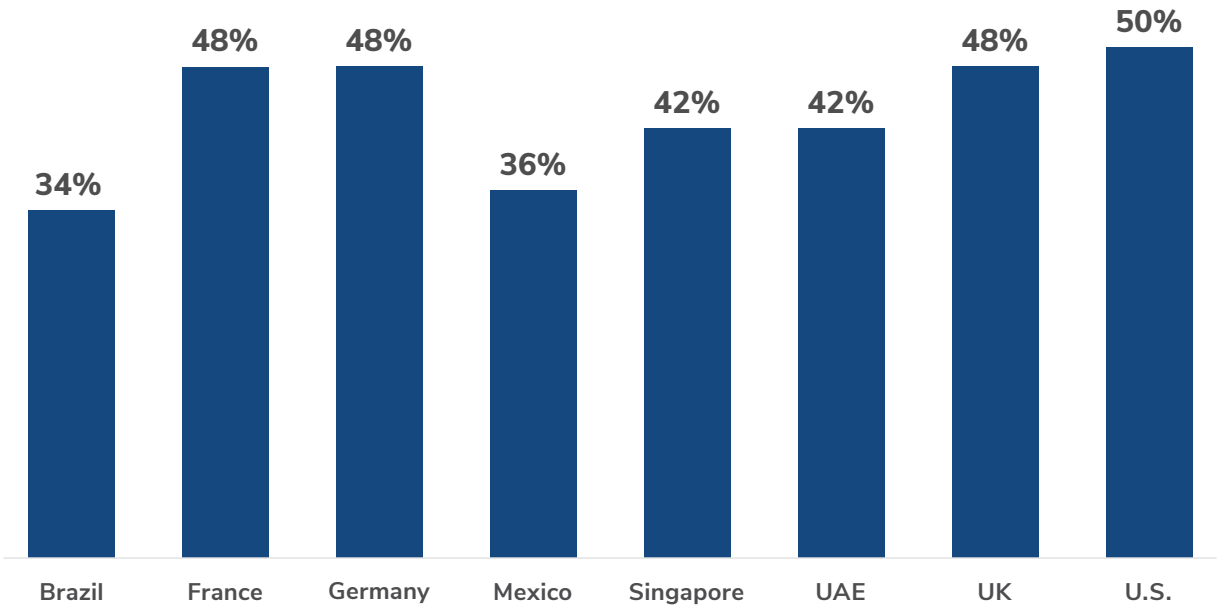
Sanctions are employed by governments as a means to change the behavior of a country, regime, individual actor or company. They can serve as an alternative means of achieving political objectives and to further the prevention of terrorism around the globe. 2022 saw a dramatic increase in the number of sanctioned entities and individuals, along with further dedication of resources by sanctioning bodies to prosecute non-compliance. In a significant development last year, the Office of Foreign Assets Control (OFAC) under the U.S. Department of Treasury imposed its largest fine of USD 24 million in the past three years. This penalty came as a result of a joint resolution between OFAC and Financial Crimes Enforcement Network (FinCEN), targeting cryptocurrency company Bittrex, Inc. Such cases demonstrate the potential financial and reputational consequences for noncompliant entities. With sanctioning bodies continuing to invest in their investigative and prosecutorial functions in 2023, we should expect to see enforcement actions and settlement amounts increase in 2024.

Sanctions are an integral component of anti-money laundering (AML) and counterterrorist financing (CTF) efforts. They enable governments to freeze assets, restrict access to financial systems, and impose penalties on individuals and organizations involved in illicit activities.

Developing resilience within a company's customer base and supply chain is critical when determining where to allocate resources to enhance sanctions compliance programs. By identifying potential vulnerabilities and implementing effective controls, companies can better manage risk and respond to evolving regulatory landscapes.

Navigating the complex world of sanctions compliance is a significant challenge for multinational corporations. In our global survey, 44% of respondents identified geographic consistency as the top challenge for sanctions compliance programs, followed by privacy protections (39%), keeping current with changing regulations (34%), and accessibility of technological solutions to support sanctions screening (33%).

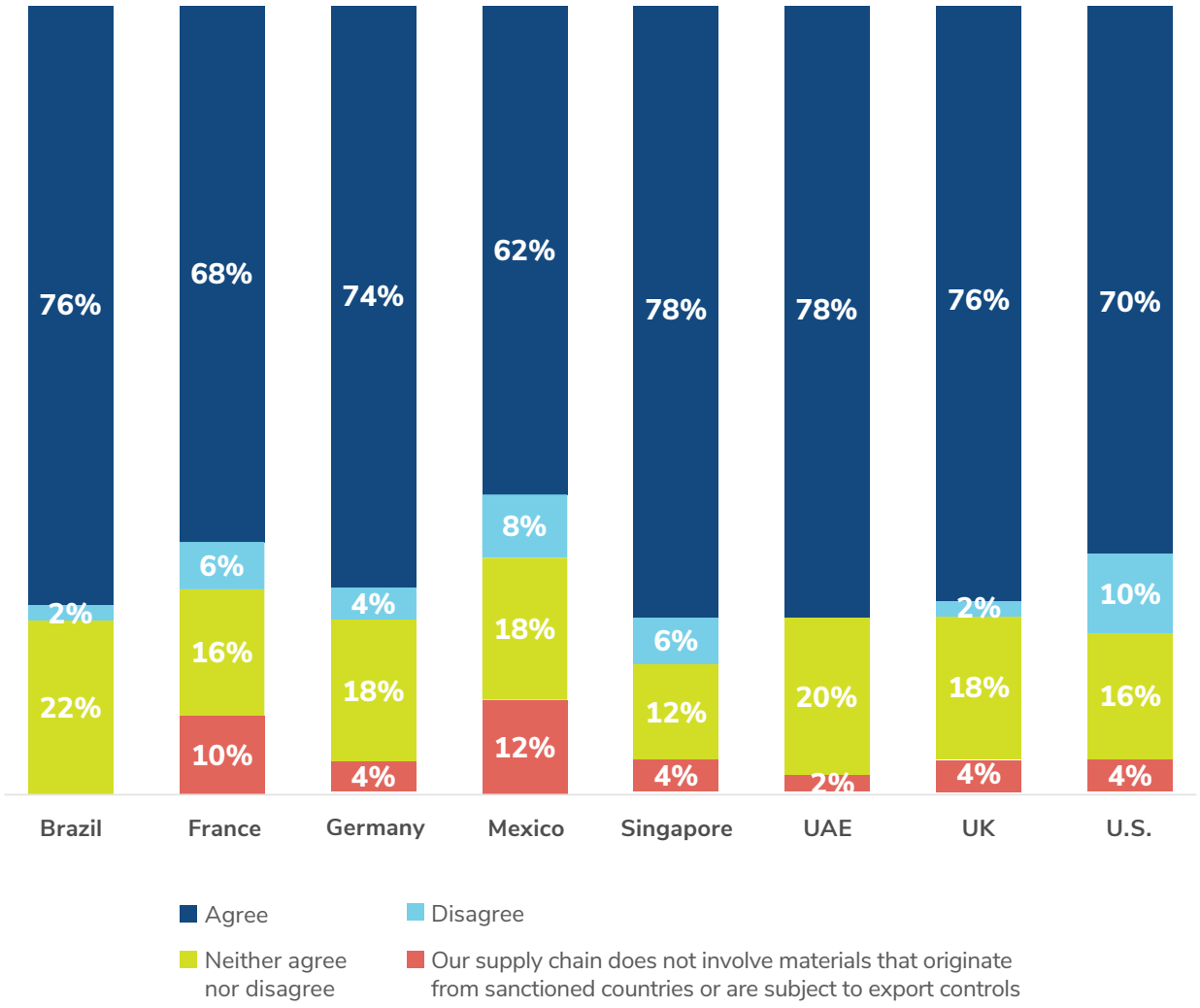
Geographic Consistency as the Top Challenge with Sanctions Compliance



Multinational corporations and banks must contend with varying sanctions regimes, each with its own nuances and enforcement approaches. While there may be general consistencies between international regulations, the differences lie in the details. For instance, the U.S., UK and EU have differing approaches to aggregating ownership for sanctions risks, leading to situations where a beneficial owner may be indirectly sanctioned in the U.S. but not in the UK. This challenge of geographic consistency is further underscored by the survey respondents in the U.S. (50%), the UK (48%), Germany (48%) and France (48%), each citing it as a top challenge at a greater magnitude than other surveyed countries.

Despite these disparities, companies are expected to comply with all applicable sanctions regimes.

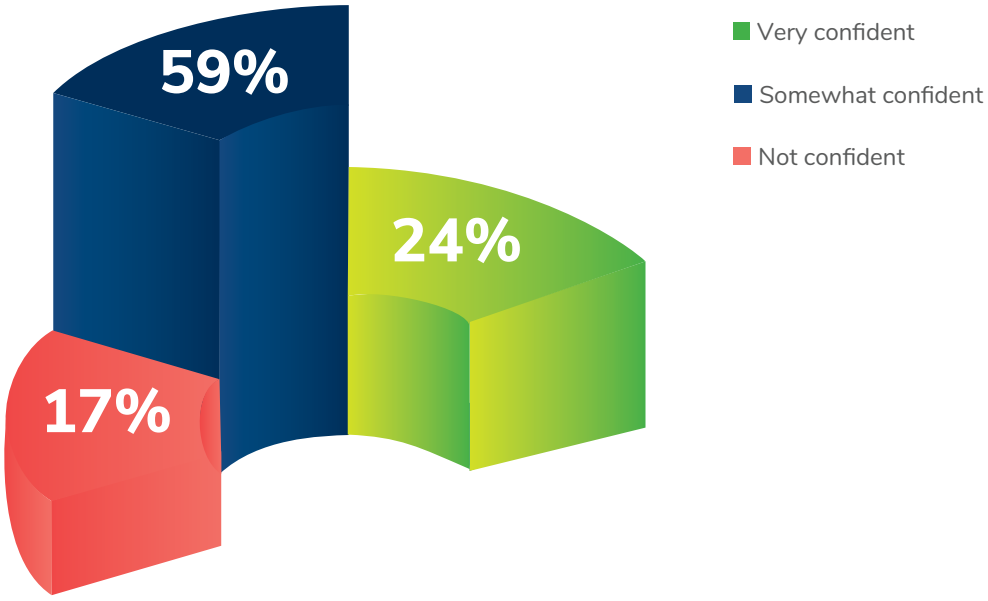
Enhancing Controls Due to Sanction Risk



To address the challenge of geographic inconsistency, two critical steps must be taken. First, international sanctions regimes should work toward aligning their laws, guidance and enforcement. Second, the private sector needs greater support from governments through increased cooperation and access to corporate information. Survey respondents expressed cautious optimism that such support will materialize in the coming year, with 52% expecting increased cooperation between regulators and financial institutions and 61% anticipating greater corporate transparency requirements.

Russia's war on Ukraine led to a massive expansion of sanctions programs, forcing organizations to rapidly adjust their risk management postures. According to our survey, 73% of global respondents plan to dedicate more time in the next year to enhancing their supply chain controls or diligence due to direct or indirect exposure to materials that originate from or are subject to export controls. This response may indicate that global supply chains have not fully shifted away from suppliers, raw materials, products or jurisdictions with heightened sanctions risk. Alongside this enhancement of supply chain controls, 67% of respondents plan to invest in technology to address the expected increase in financial crime.

Confidence in Support of Their Supply Chains



Despite plans to enhance supply chain controls, 83% of global respondents expressed confidence that their supply chains are sufficiently supported and resilient to prevent, identify and mitigate sanctions risks. This raises the question: will they be prepared for the threats of tomorrow?

Future-Ready Sanctions Compliance Programs

Russia's war on Ukraine has shed light on both historic and new sanctions evasion methods. Historically, these methods have included documentation fraud, obscuring or falsifying ownership, and other classic smuggling tactics. However, new methods have emerged, such as the greater complexity of ownership behind impenetrable corporate veils in offshore jurisdictions, adding ownership layers in various countries and the pervasive use of intermediaries. Some evaders are also sheltering assets in jurisdictions out of reach of sanctions regimes. And in limited situations, such as the OFAC sanctioning of Tornado Cash in August 2022, sanctions evaders are utilizing cryptocurrencies and virtual currency mixers.

These new sanctions evasion methods may be linked to the sentiment shared by many that there are ongoing data gaps caused by limited corporate transparency laws. Information sharing among allied nations with sanctions regimes, such as the multilateral Russian Elites, Proxies and Oligarchs (REPO) task force, has been crucial in closing these gaps. However, challenges will persist in countries where there is no current or planned effort by governments to create a publicly accessible corporate registry with validated ownership information. To address these challenges, sanctioning bodies recommend that companies conduct an appropriate level of due diligence, including source of funds or wealth checks.

Future threats include public conversations suggesting that sanctions on Russia have led to unintended blowback against the U.S. dollar by creating alternative financial systems. While economic experts believe there is limited, if any, prospect for the U.S. dollar to be unseated as the world's reserve currency, these alternative financial systems nonetheless pose unique challenges to sanctions and export controls professionals.

Russia's war on Ukraine was viewed by some as the Black Swan event of 2022, an extremely rare and unpredictable event, but may seem obvious in hindsight. Preparing for such Black Swan events is a difficult task but a useful exercise in creating resilient sanctions compliance programs, particularly now that corporate crisis management programs have begun conducting table-top exercises for similar sanctions-relevant world events. Companies may want to consider if they are prepared should the U.S. sanction other countries at a similar scale as they have Russia.

How Companies Must Respond

In order to stay ahead of the evolving sanctions landscape, companies must shift their perspective on sanctions compliance programs, recognizing them as dynamic frameworks requiring regular upkeep and maintenance. A uniform approach centered around a single nation's laws is inadequate for multinational organizations. Instead, a customized compliance program should reflect the laws of each operational jurisdiction in addition to international enforcement bodies. An effective sanctions compliance program should align with a company's corporate culture, geographic diversity and business practices, supported by knowledgeable employees.

This approach may be seen as a luxury or a lofty pursuit for cost-constrained compliance programs; however, changing the organization's mindset around sanctions compliance as a competitive advantage that enhances the value of the company is essential to mitigate regulatory and reputational risks. To achieve this, companies can adopt best practices such as tailoring their sanctions compliance program to reflect local culture, business practices and laws, in addition to international laws. Utilizing enhanced corporate data sets for greater data on ultimate beneficial ownership and incorporating risk assessments, training, testing and top-down support can further strengthen compliance programs.

Technology also plays a vital role in enhancing and supporting sanctions compliance efforts. Specific technologies that have proven effective include transactional sanctions screening software, particularly those enhanced by machine learning, and integrations between procurement or vendor onboarding platforms that incorporate automated sanctions screening. Tools that can rapidly process data, enrich data, identify linkages to high-risk data and integrate information from various sources have become indispensable in managing the complexity of sanctions compliance. As the use of virtual assets expands, blockchain analytics solutions are increasingly being incorporated into company controls, such as customer due diligence, transaction monitoring and sanctions screening for companies exposed to virtual assets. These innovations should continue to drive developments for other blockchain use cases for non-cryptocurrency-exclusive applications such as smart contracts in the months ahead.

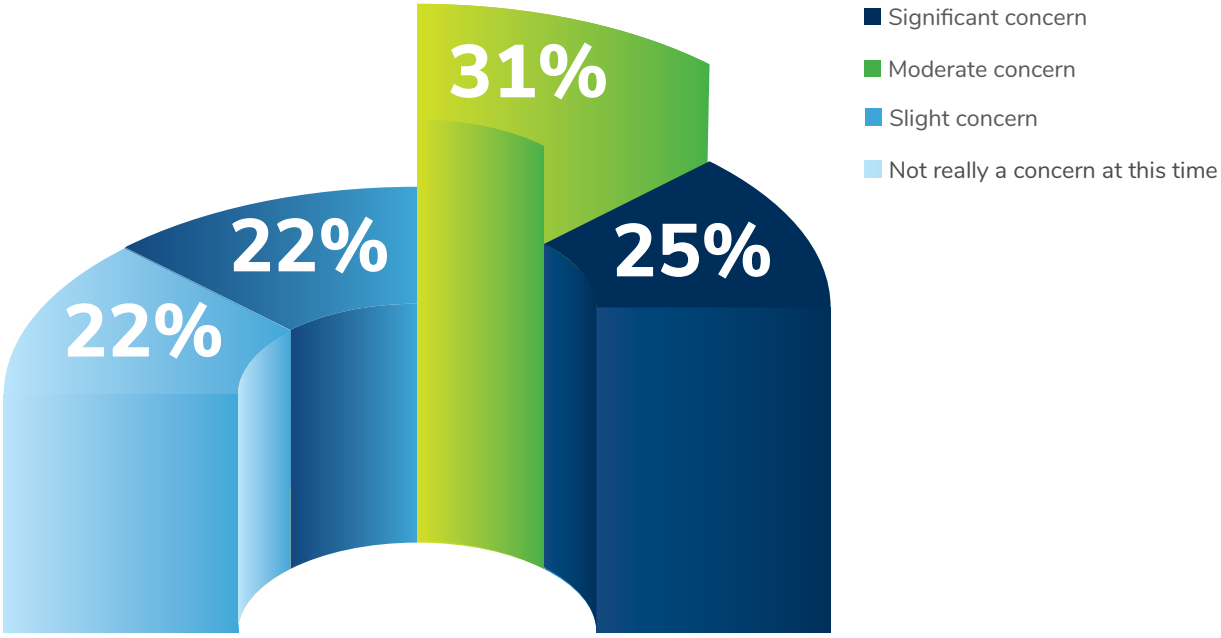
In conclusion, the future of sanctions compliance programs will rely on companies adopting a proactive and dynamic approach and leveraging technology, best practices and international cooperation to effectively manage and mitigate sanctions risks. By doing so, organizations can remain resilient and adaptable in the face of changing geopolitical landscapes and regulatory requirements, ensuring their continued success in the global marketplace.

The Challenge of Crypto and Financial Crime

by Haydn Jones

There are a variety of risks that need to be considered in the case of crypto—market, regulatory and cyber risks to name a few—but the most lethal is a transaction potentially linked to financial crime, whether suspected or actual. It's imperative to understand how a risk profile changes through the entire lifecycle of the transaction; it could get better with no link or it could get worse. Interestingly, our survey indicates that cryptocurrency risks pose an immediate concern to only 56% of respondents.

Financial Crime Risk Posed by Cryptocurrency is a Concern to 56%



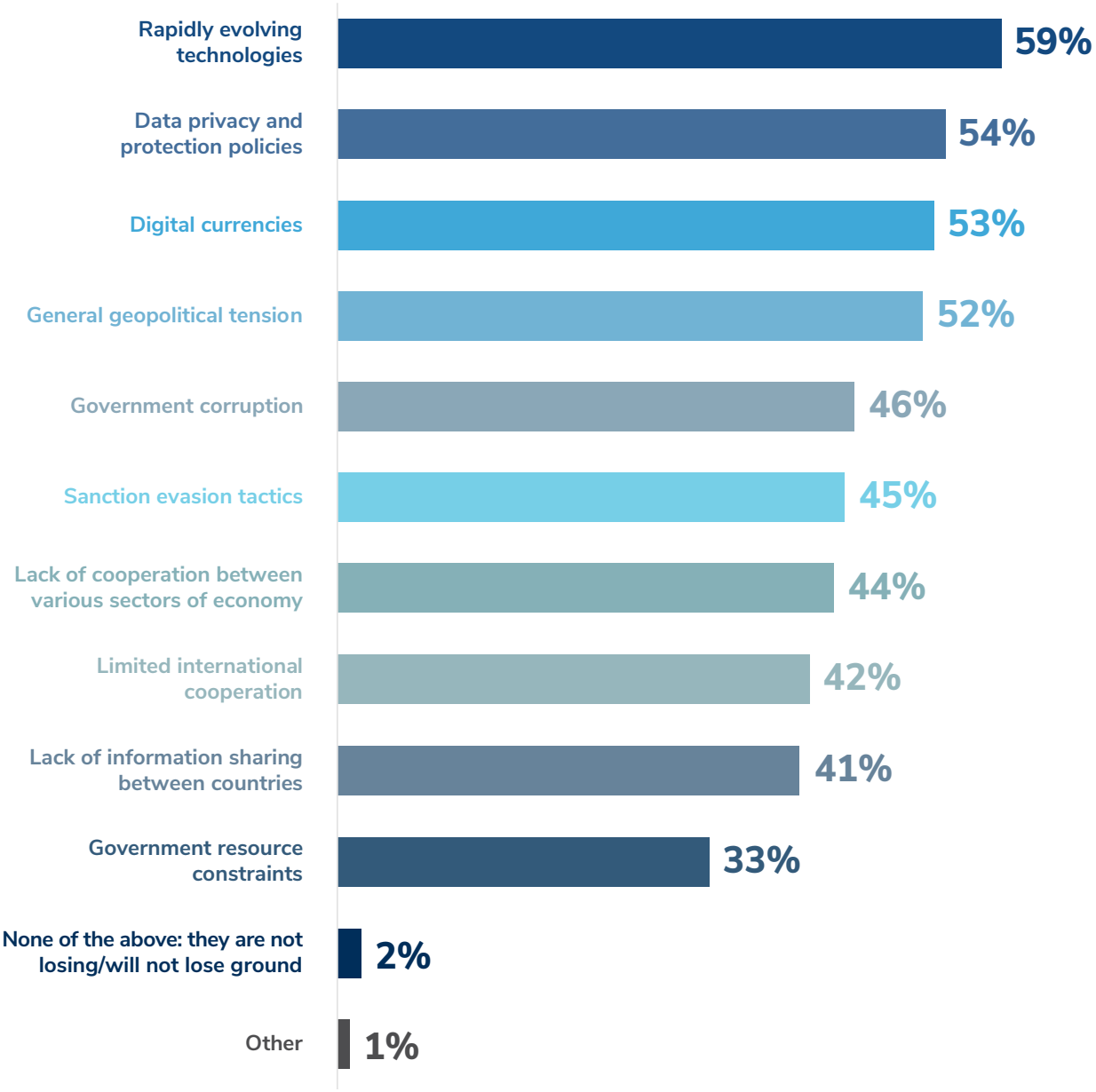
The subsequent challenge of further understanding the financial crime risk is then one of monitoring that risk over three very different worlds—traditional finance, crypto and financial crime—and then connecting the dots across those three worlds to highlight activity which gives us cause for concern. Regrettably, there are many different scenarios in how crypto is used, both good and bad, and it's only through policing the bridges between these three worlds, and monitoring what's going on inside them, that we gain further insight into whether the circumstances are legitimate or otherwise. For example, a crypto day-trader would be expected to demonstrate that the movement of funds between crypto and fiat happened within a fully regulated perimeter, with proper know your customer (KYC) and anti-money laundering (AML) provisions, suggesting the risk or link to illicit activity was low. However, a scenario where a bank with payments to and from customers' accounts, which are then transferred into an unregulated crypto exchange and then onwards via a crypto

with enhanced anonymity, would give major cause for concern as linkages to illicit activity can happen with ease. While the outcome is different in each scenario, both cases suggest three areas of focus to provide some structure for our risk profiling activity:

1. **What crypto is involved in the transaction and how is it being used?**
2. **What are the related crypto entities?**
3. **What is the end-to-end regulatory status?**

Incidentally, the first point is cited in our survey data with at least half of respondents, amongst other things, highlighting that digital currencies pose a challenge to government in fighting financial crimes.

What are the Top Challenges a Government Faces in the Fight Against Financial Crime?



What is Crypto?

Crypto is a broad term used loosely to describe the technology that has led to a means of transmitting value via a shared or distributed ledger, which can be accessed publicly or, in certain cases, privately. Since this is codable technology, the nature of the value that is captured and transmitted is limited only by the imagination of those who design it. For example, crypto technology can be used to reference digital coins that can act as a store of value, such as bitcoin, or reference existing types of value, such as securities, or money held in conventional bank accounts. Crypto can also reference artwork, for example, non-fungible tokens, or provide access to storage or computing capability, with so-called utility tokens.

In the context of financial crime, and like conventional money, all types of crypto can be used for or linked to criminal activity. However, crypto has some interesting features which make monitoring and detection of wrongful activities easier, as compared to traditional money. Because there is a shared public ledger, crypto is generally traceable, and a transaction history can be compiled which enables attribution of a hygiene rating to transactions. Where criminal activity is proven, or suspected, such as in a hack or a ransomware attack, we can link those events to the related transactions, effectively in perpetuity, such that they will always be tainted with that activity. There are means of obfuscation through tools such as mixers which can conceal a coin's history, but these are usually detectable and would trigger a red flag.

Alongside bitcoin, the most well-known, there are another 24,000 cryptos, or digital assets, many unique and purporting to exhibit some special features which make them stand out from the rest.[1] In broad terms, crypto segments into stablecoins, utility tokens and exchange tokens. Stablecoins are generally backed by a deposit held in a bank. Utility tokens are used for accessing a service of some kind. Exchange tokens, such as bitcoins, are used for payments, although their volatility can make them attractive to investors. Certain types of crypto can be categorized as enhanced anonymity coins, which as their name suggests, have features which disguise origin and transaction value. Aside from enhanced anonymity coins, digital assets are not completely anonymous; they are, rather, pseudo-anonymous. As soon as they touch an entity which has proper record of customer details, such as a regulated crypto exchange, then it should be possible to attribute identity information to the relevant transactions, provided the records have been held correctly and are accessible.

However, there's a catch we see with the enhanced anonymity coins. In cryptography, there are lots of ways to anonymize transactions and make them difficult to trace. When cryptography is applied to conceal the identities of originators, beneficiaries and values being transferred, alarm bells need to be sounded. This is not generally the case with bitcoin; because the transaction history is captured on a public ledger, we can develop a profile, or hygiene rating, of bitcoin transactions. Provided we know whether certain of the bitcoins were used for bad things, we can attribute a "badness" rating to those transactions. This is very helpful for tracing activities related to financial crime. This is not the case with enhanced anonymity coins and, if linked to an individual, entity or transaction, should trigger a red flag.

Finally, because this crypto technology is programmable, we see huge growth in innovation in how the technology is developing. For example, the so-called decentralized finance (DeFi) protocols allow one class of asset to be locked in exchange for another class of asset. This ability to swap asset types is very common in traditional finance, hence the reason why DeFi is interesting in providing similar types of services in the world of crypto. However, DeFi protocols also represent a major risk in being able to bridge from one asset to another, one of which may be illicit whereas the other is ostensibly untainted.

Understanding the nature of the crypto involved in a transaction, the extent to which it is traceable and the rationale behind why it is being used is the start point in assessing a transaction risk profile.

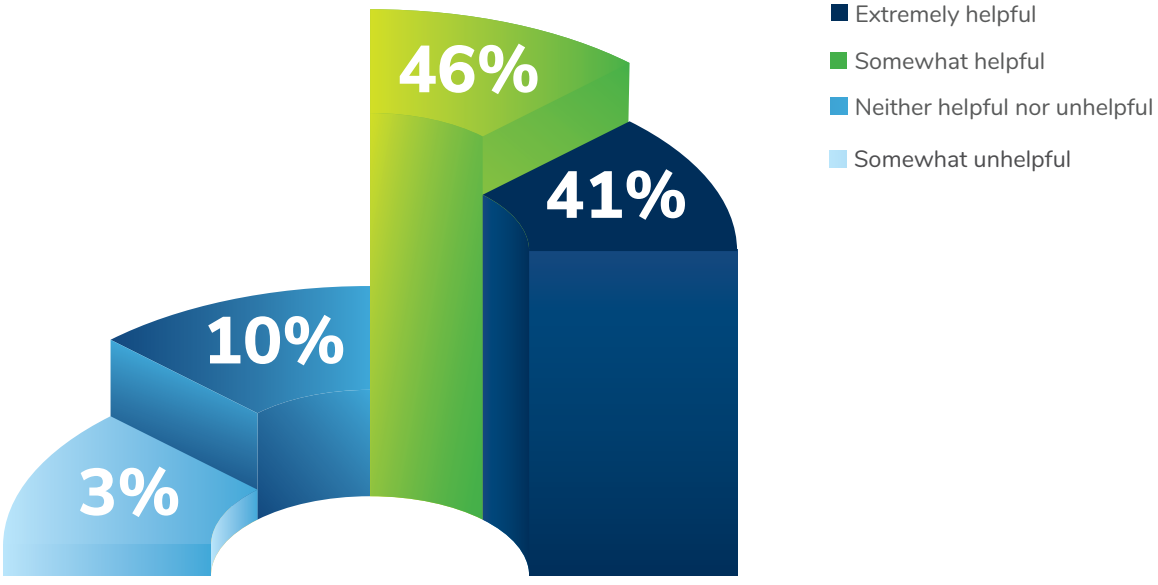
1. https://coinmarketcap.com/

What are Crypto Entities?

Crypto activity is generally centered around exchanges, custodians, wallet providers and issuers. Crypto exchanges, of which there are more than 600 globally, allow parties to buy and sell crypto for other forms of crypto, such as bitcoin or stablecoins, or fiat, such as USD or Euros. Custodians hold crypto on behalf of third parties, very similar to the role of banks in holding deposits for their customers. Wallet providers allow self-custody, where the individual or beneficial owner of the crypto concerned has complete control, as opposed to a custodian, where control in part vests with the custody provider. Issuers, as the name implies, issue crypto currency, the design of which depends on the features the issuer is seeking to exhibit.

There are two other classes of entity which need to be borne in mind—crypto automated teller machine (ATM) operators and crypto miners. Crypto ATM operators allow physical cash to be exchanged for crypto. The risks associated with money laundering should be immediately apparent and, as such, there are strict regulatory frameworks for ATM operators. These essentially provide for the capture of identity and verification information as it relates to cash being exchanged for crypto, and vice versa. For example, in the UK, all crypto transactions executed via a crypto ATM above GBP 150 require KYC verification. The second class of entities are the crypto miners who provide the computer power which runs the crypto network, in return for which the operators receive units of crypto, for example, bitcoins. The computing units themselves are expensive and energy hungry. However, they have the advantage of generating new, or untainted crypto, such as bitcoin, and therefore represent an effective means of converting cash gained via illicit means. That cash is typically deployed to purchase the miner hardware or pay for energy. Dirty cash in, clean crypto out. Crypto miners are also generally unregulated, albeit they are banned in certain countries. For countries where miners are unregulated, this means their activities don't need to be registered. As such, they represent a potentially invisible bridge between illicit funds and clean crypto. However, to detect this we have the advantage of the public ledger, which allows us to observe the distinctive pattern of transactions a miner generates. This in turn may point to the illicit conversion of funds into untainted crypto. It may also just be an indicator of legitimate mining activity and so research and deeper inquiry is essential through profiling the beneficial owner. Opaque structures, with poor explanations of the source of wealth, usually point to questionable arrangements in relation to the underlying activities. Here, a register of beneficial interests is vital, a point clearly highlighted in the results from our survey.

Beneficial Ownership Registry is Helpful to the Vast Majority of Companies Surveyed



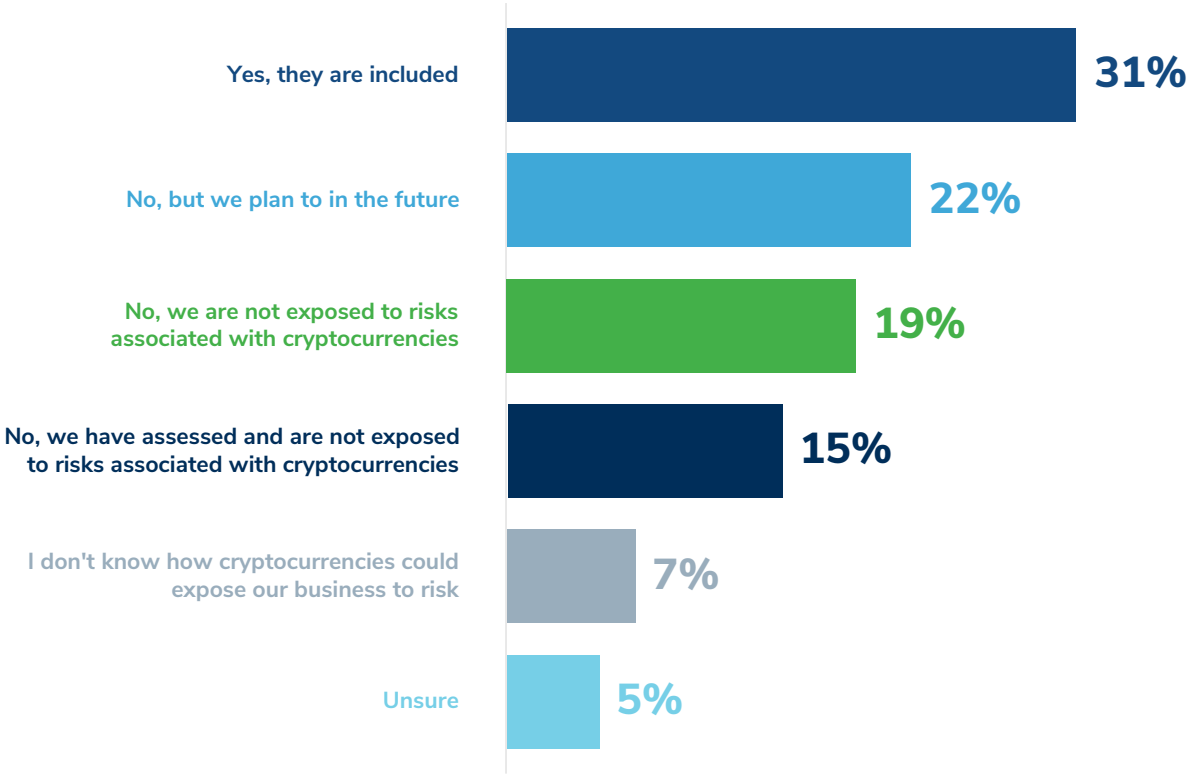
What is the End-to-End Regulatory Status?

The extent to which crypto is regulated varies country by country and continues to evolve. Some jurisdictions are well down the path of regulating crypto, whereas others have yet to start. Understanding the regulatory status of a particular crypto or a particular entity is an important starting point when considering the overall hygiene of a transaction and the risk of being linked to illicit activity of some kind. Unfortunately, it doesn't stop there. Being guided by a simple regulatory stamp of approval is generally insufficient. It is important to understand what concerns or issues a regulator may have open with a particular entity and, in the spirit of propriety, its good practice to request from the entity concerned information, such as the latest Money Laundering Reporting Officer (MLRO) report, the last regulatory filing, or policies for onboarding customers. Reducing the risk of financial crime is about detecting and removing gaps in the entire regulatory perimeter, extending across into traditional finance. Any such gaps can have serious consequences. Understanding where the gaps are, and the steps taken to either mitigate or remove the risk entirely, is a core principle of our framework.

Depth and breadth of recordkeeping is essential. Given the ease with which funds can be moved between crypto and fiat, sources of wealth should underpin any risk analysis. Regardless of the structure, the identity and profiles of the beneficial owners need to be understood, extending diligence activities proportionately as necessary. Reference to beneficial ownership registers is again obviously paramount, as evidenced in our survey.

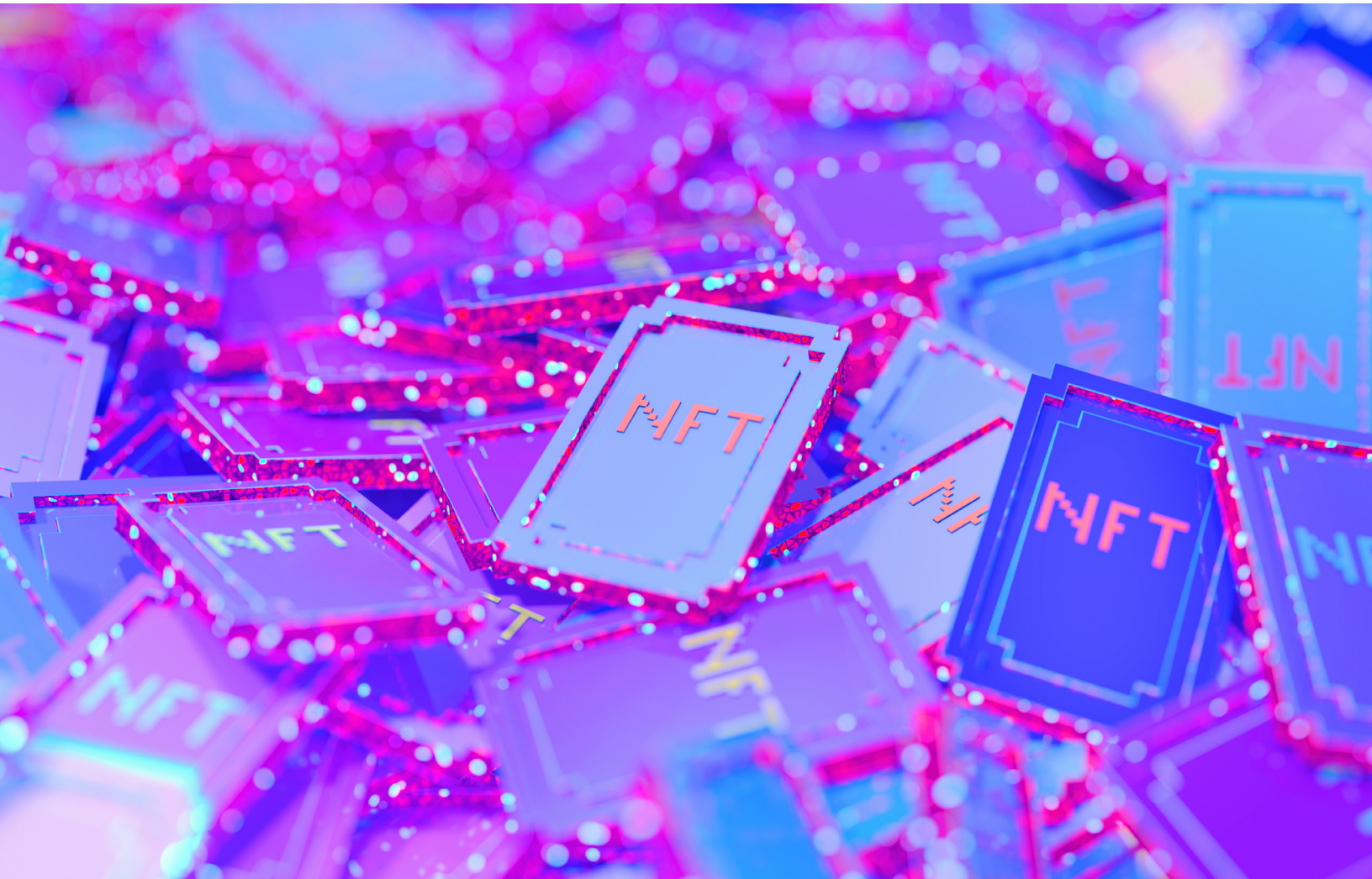
This holistic view of the transaction is essential. Nearly one-third of survey respondents indicate that their companies' financial crime compliance programs cater to risks associated with cryptocurrencies, with 22% reporting they are planning for future crypto risks. This is encouraging, but there is still clearly work to be done.

One-Third Indicate Financial Crime Compliance Programs Cater to Organization's Cryptocurrencies Risks



Summary

In some ways, with the readable and relatively straightforward public ledger technology, the features for detecting and pursuing illicit crypto activity are superior to those of conventional money. What our survey highlighted, however, was the lack of understanding. One in four respondents stated that the financial crime risk posed by cryptocurrency is a significant concern, and more than 60% of respondents stated that understanding the risks associated with crypto is a key challenge. Given the utility of the technology and features which improve the ability to fight financial crime, especially the moves by central banks to adopt similar forms of the technology, crypto is arguably a form of money that is very much in our future. We need to understand it, the frameworks that make it safe to use and the ever-changing regulatory landscape around it. And with the advent of freely available and sophisticated AI tools which can automate the transfer of crypto and obfuscate its use for illicit activities, sophisticated frameworks to monitor and detect for the risk of illicit activity using this technology will need to become ubiquitous.



Data as the Critical Factor in Fighting Financial Crime

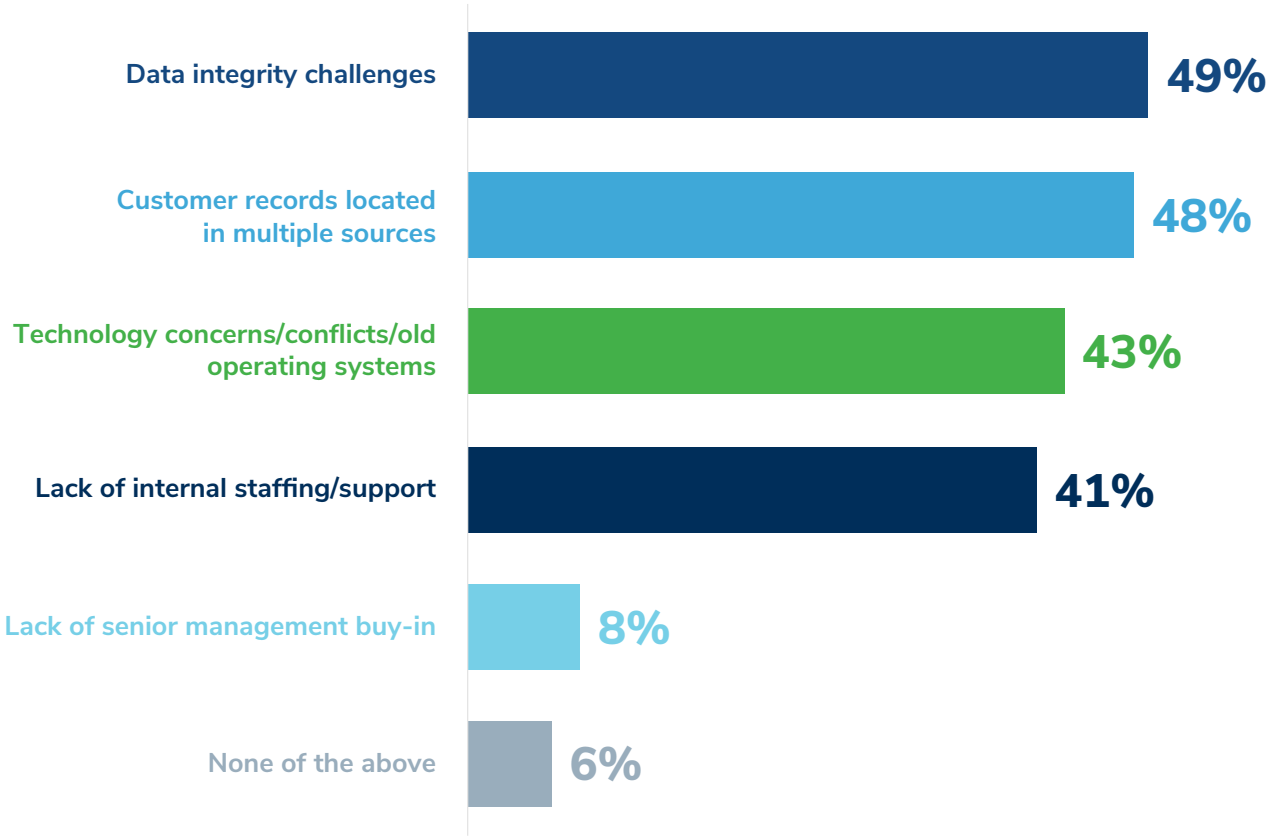
by Haydn Jones

There's a saying attributed to W. Edwards Deming, the father of the mid-1980s quality movement: "In God we trust. All others must bring data." It can hardly be truer than when applied to the challenge of fighting financial crime and the relevance of accessing the right data at the right time. While outwardly simple, safely taking the right bits of data from your data warehouse (or lake) and then carefully examining them for insight brings with it many latent and deeply engrained challenges. If the task is done incorrectly, it means the wrong people are potentially on the loose and free to do bad things. If done properly, it can maintain—or even build—brand value.

Much of the challenge relates to the growth of the imperfect organization consisting of many different legal entities and different applications, acquired and patched together over the course of different mergers and acquisitions. Disposing of part of an organization can also result in compromises, especially where some core piece of data processing has been tactically routed through the departing organization as part of a short-term fix. Financial services is a case in point, which ironically sits at the center of the financial plumbing that moves money around the world. Much can be said for newer, simpler organizations, although they can suffer from a lack of experience, immature culture and a rush for growth, all of which potentially lead to cut corners.

For established organizations, the cloud offers an efficiency opportunity, but it doesn't necessarily solve the data integrity challenge. Poorly organized data, ported from a legacy environment into the cloud, is not the answer. Using data to fight financial crime starts with the integrity and consistency of records across multiple systems, whether in the cloud or on legacy platforms. The maintenance of client static data might be the least glamorous of the data challenges, but having centralized control of a client's static data change requests can go a very long way to understanding volume and consistency across different systems. Being able to measure consistency of client identifiers across different processes is the starting point, as it provides a metric to measure client data integrity. In developing this, some of the key questions that need to be asked are: How many systems have client data? What is the mapping and consistency across these different systems of the different client identifiers? What is the governance process for making change happen? Ownership by a senior leader, such as a Chief Data Officer (CDO), is essential, as is locking down systems in relation to changes that are made to client static data. The CDO sets the tone for data culture, with their management attention being essential. And the data from our survey appears to echo this, with only 8% of global respondents citing lack of senior management buy-in as a concern. The follow-through and discipline on these efforts, however, matter most.

Challenges in Implementing Technology Solutions to Support Core Client Life Cycle Processes

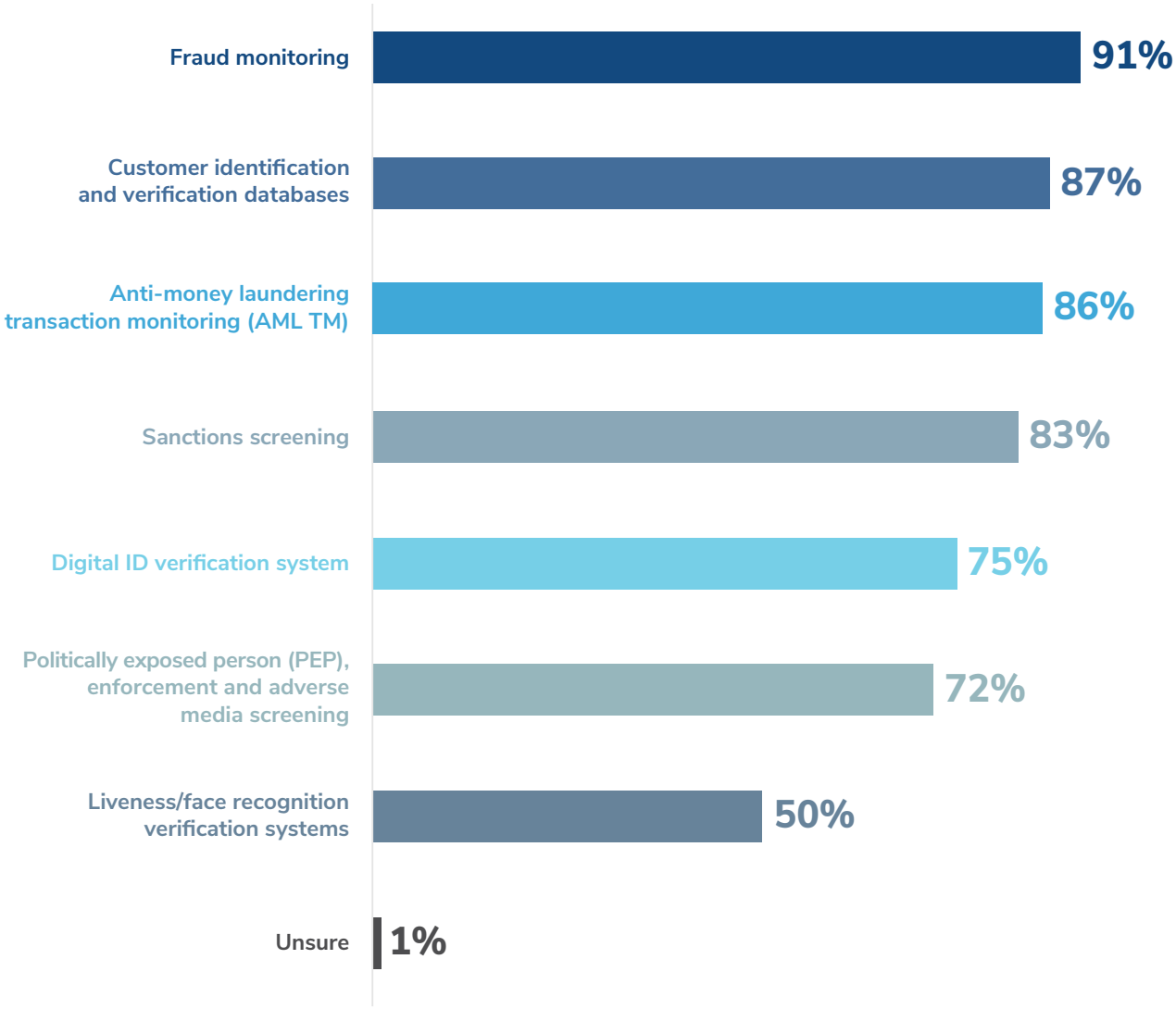


An IT strategy needs a data strategy. Data should be stored once and only once. Typically, it is only when data is being moved or replicated across an organization that breaks within data integrity begin to arise. The data strategy needs to be supported by a data governance framework central to which is a data strategy steering committee. The committee should be staffed with experienced people who are equipped to ask the right questions and authorized to make decisions and request that resources are deployed as required.

More broadly, the data challenge can also flow from a lack of an IT strategy. IT strategies tend to be verbose and difficult to understand. At its simplest, an effective organization-wide IT strategy should categorize systems into one of three categories: retire, maintain, or invest. The organization should be posing questions as to which systems are strategic, which are for retiring and which are in a holding pattern. The decision to keep or retire a system is a function of cost, break/fix performance, data utility, functionality and alignment to strategic hardware and software standards. Unfortunately, decisions take time, and this is a complex area, which is often overlooked, to the organization's cost.

The data challenge is also not uniquely internal. Financial services are highly regulated, with intersecting Venn diagrams of requirements that need to be met, combined with regulators demanding high degrees of compliance. Much of this external data covers fraud monitoring, customer ID and verification databases, anti-money laundering transaction monitoring (AML TM), sanctions screening, digital identification systems, politically exposed person (PEP) enforcement and adverse media screening. Our survey results show the extent to which external data sources are used, with fraud monitoring and customer identification ranking highest at 91% and 87% respectively. Changes made in these data sets must be tracked and governed and will also require the involvement of supplier management teams and will be subject to some level of regulatory oversight.

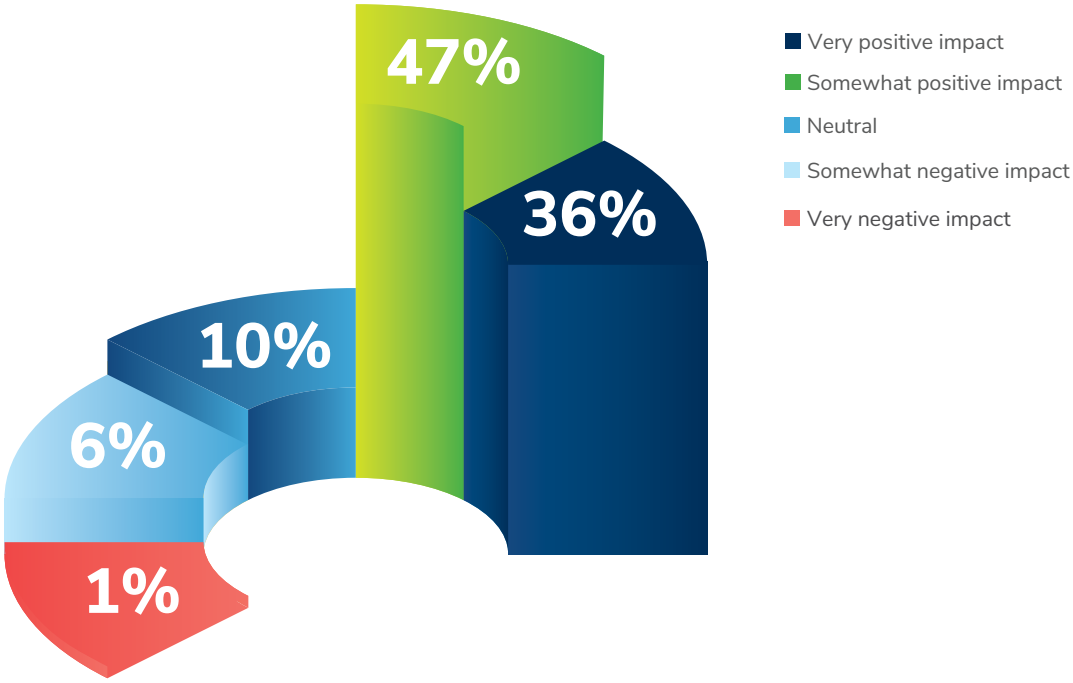
Which of the Following Financial Crime Tools are Most Commonly Used?



The Importance of Data Hygiene

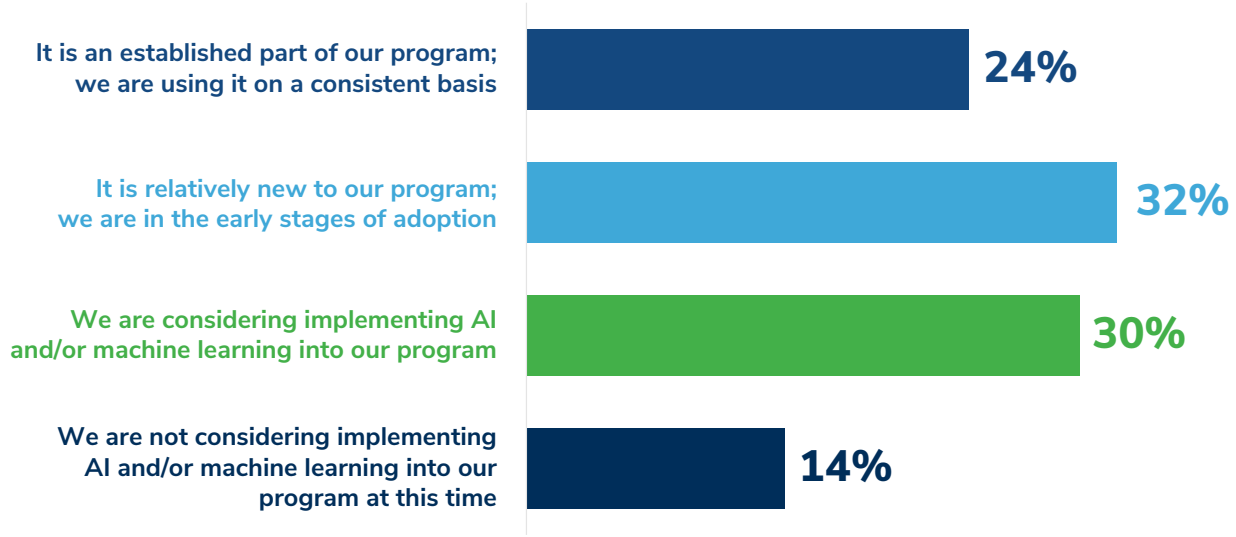
Good data practice is about fostering a positive culture of data stewardship. Recognizing the importance of the data narrative and understanding the flow of data across the organization's technology and how it ties to regulatory oversight and operational risk is essential. This is reflected in our survey results, with more than two-thirds of respondents planning to invest in technology and 60% expecting to increase their cybersecurity budgets to improve their data perimeter. Ironically, most organizations are driven by quarterly sales targets and not data, albeit the latter is essential to support the former. Data issues only ever arise when there is a mistake, an audit or a change event. But bad data goes to the bottom line, either in the form of operational errors and the cost of restoring them, regulatory capital, or fines. Good data practices come from the top of the organization, with a zero-tolerance approach to bad data similar to the way that the Six Sigma quality movement drove out manufacturing errors. The challenge is cultural, requiring strong data stewardship that is visible and transparent. Organizations are generally more comfortable rewarding performance for meeting sales targets or customer satisfaction than recognizing the team with the cleanest static data.

Perceptions Towards AI as Part of the Monitoring Process is Very Positive



All of this will become even more pressing with the advent of AI, all of which is driven by data. Encouragingly, despite a cautious, and in some cases even alarmist, commentary emerging in the media, perceptions toward AI as part of the financial crime monitoring process are overwhelmingly positive per our survey. The challenge is well suited. Fifty-six percent of respondents reported that some form of AI had been implemented into financial crime compliance programs, albeit recognizing that AI is still relatively new in the majority of these cases. Whether this starting point is a baseline trend will take time to emerge, but with more than one in two reporting some level of AI implementation, this is a data point that cannot be ignored.

Implementation of AI Solutions as Part of Current Financial Crime Compliance Program



In summary, what was most encouraging from the survey was that at least two-thirds of respondents were using technology to screen for customer regulatory actions, law enforcement and sanctions. But that still leaves a gap of one in three which presents a latent risk which could be avoided by supporting technology. Technology gives us access to data, but data discipline is essential to manage risk and run an organization. Rarely is data a glamorous topic, but much rests on it. The truth really is out there; you just need the data to find it.


SERVE NOTE
565 D
THIS NOTE IS LEGAL TEND
FOR ALL DEBTS, PUBLIC AND
JULY 4, 1776.

Caveat Emptor: The Use and Abuse of Carbon Credits

by Julianne Recine and Chris DeSa

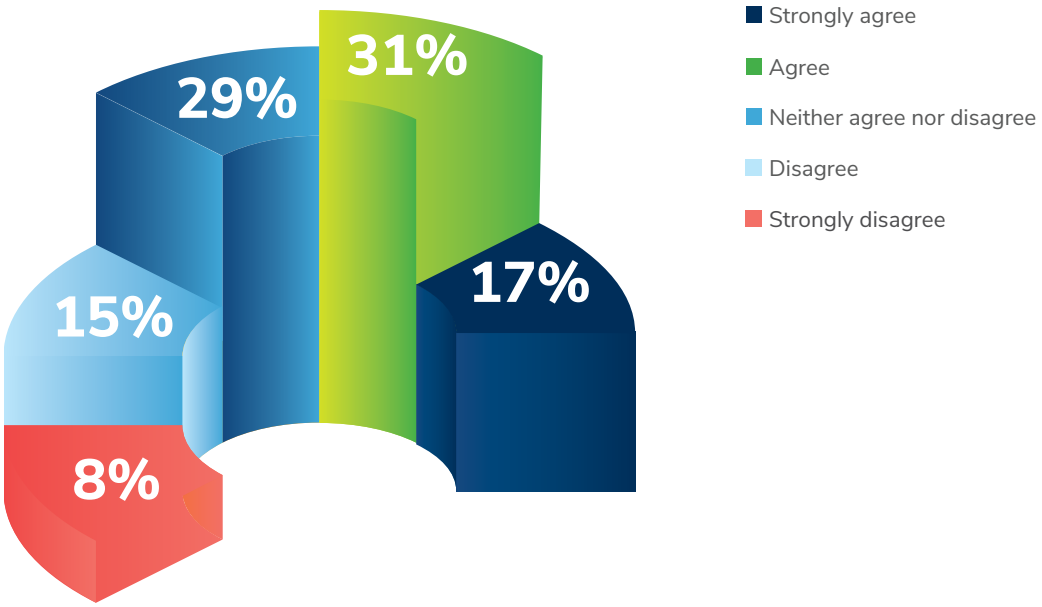
The last several years have seen a material increase in the use of carbon credits and offsets by companies as part of broader global efforts to address climate change and reduce carbon emissions. That trend will, in all likelihood, exponentially increase over the next decade. The use of carbon credits, however, is by no means a risk-free proposition. The rules remain highly uncertain and subject to frequent modification. A patchwork of opportunistic bad actors, including, in some instances, organized criminal groups, has flocked to the space. And more recently, regulators, media, civil society organizations and courts have been rightfully cracking down on the false and misleading use of credits with dubious contributions to emissions removals or reductions. Yet, despite the obvious headwinds, carbon credits can still play an important role in future efforts to manage global climate-related impacts and goals particularly considering recent efforts by standard setters and regulators (for example, in the EU, the UK, Canada and the U.S.) to actively try to address the related concerns. As this process unfolds, companies that choose to acquire carbon credits need to be especially vigilant and actively manage the related risk factors, taking proactive steps to ensure the integrity of the credits and their use.

The Potential Benefits of Carbon Credits

The terminology around carbon "credits" and "offsets" is confusing. They are somewhat ill-defined concepts and often used interchangeably despite potential differences. Generally, they can refer to formal credits generated from mandatory carbon-reduction schemes (such as cap-and-trade regimes in the EU, Australia, New Zealand, South Korea, California and Quebec) or to credits or offsets generated voluntarily under specific frameworks and standards and registered with a carbon registry. Trade in these voluntary carbon credits, with each credit being equivalent to one metric ton of carbon dioxide equivalent (CO_2e), emerged with the 1997 United Nations (UN) Kyoto Protocol to facilitate and enable carbon removal and/or reduction projects. Market mechanisms were sought to incentivize and promote projects that would not have occurred in the absence of some form of compensatory mechanism for developers. Proponents have argued that, without such compensatory credits or mechanisms, there are minimal incentives for market-led carbon reduction and removal projects—even those with clear and distinct atmospheric carbon removals like carbon capture technologies.

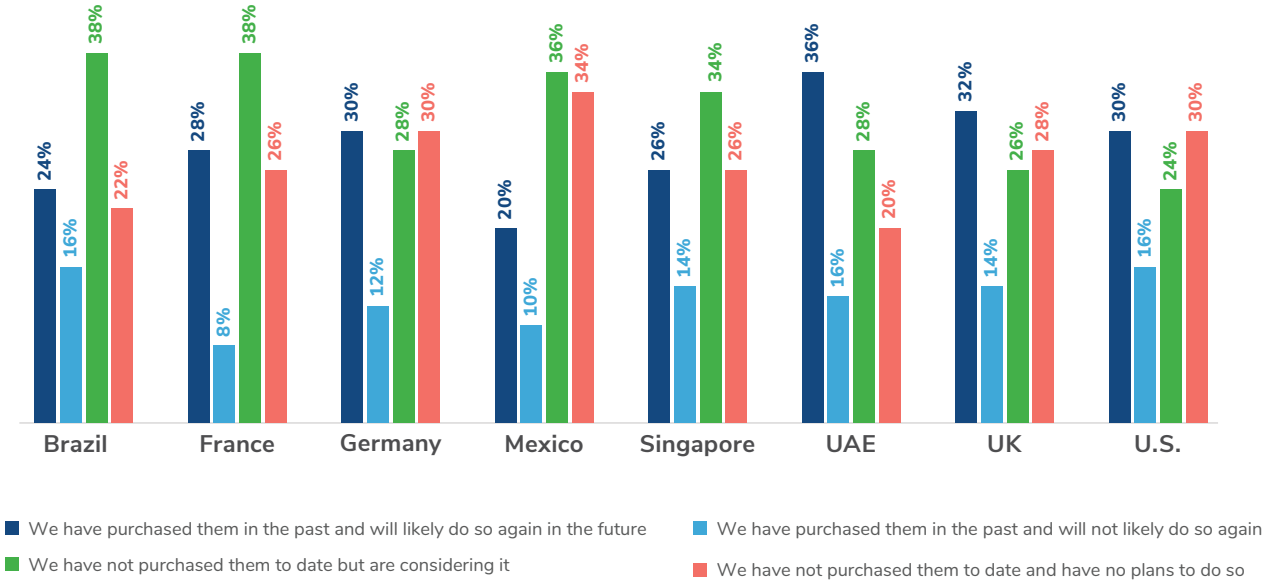
From a buyer's perspective, voluntary credits can be particularly helpful in facilitating efforts to promote climate action and neutralize residual carbon emissions where direct emissions reductions would prove too costly and difficult. Consistent with that view, 48% of survey respondents agree that carbon credits are an effective solution for fighting climate change.

Carbon Credits are an Effective Solution for Fighting Climate Change



Given the perceived utility of voluntary carbon credits by many companies and financial institutions, it is not surprising that demand has increased significantly in recent years. Most respondents (60%) to our survey have either already purchased some form of carbon offsets (28%) or are considering purchasing them in the future (32%).

Who is Buying Carbon Credits?



And the use of credits is only expected to grow in coming years for three interrelated reasons. First, evolving global regulatory disclosure requirements around greenhouse gas (GHG) emissions, especially in the U.S., the EU, the UK, Canada and Australia, means that corporate emissions—which have largely gone unmeasured or hidden from public scrutiny until recently—are now being made public. Second, the

increasing use and integration of overall environmental, social and governance (ESG) factors, including emissions data, into investment decision-making means corporate management is increasingly attuned to their relative performance and reputation on emissions factors vis-à-vis competitive benchmarks. Third, companies are increasingly embracing detailed energy transition plans to reduce their carbon emissions and impact, including direct actions to lower climate emissions reductions and other intermediate means (such as climate credits) to "neutralize" residual emissions.

There's No Free Lunch: Carbon Credits Are Not Risk-free

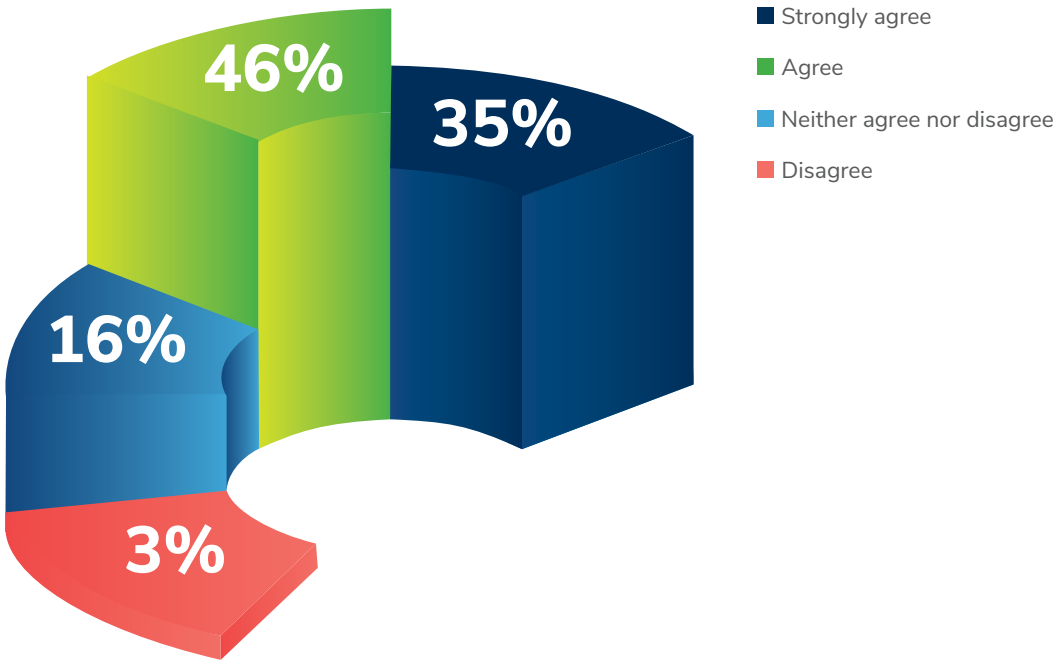
However, despite the many potential benefits and merits of carbon credits, the current uncertainty, lack of definitive guidance and regulation around accounting mechanisms and the patchwork of organizations involved means companies should proceed with caution.

Companies should be especially mindful of three related risk factors related to carbon credits: third-party and jurisdictional issues; project accounting and impacts; and disclosure and communications risks.

Third-Party and Jurisdictional Risks

First, the opacity and complexity of carbon credit markets has resulted in numerous opportunistic and dubious third parties flocking to the industry. That includes organized criminal groups, corrupt politicians and a slew of other potential bad actors. Companies that purchase carbon credits should vet and screen the widest possible swath of individuals and organizations associated with carbon credit offerings and projects to the fullest extent practicable. Most respondents to our survey appear to understand the necessity with 82% agreeing they already do or will conduct due diligence to ensure carbon credits are purchased from a legal entity.

Organizations That Agree to Conduct or Will Conduct Due Diligence to Ensure Purchased Carbon Credits are From a Legit Entity



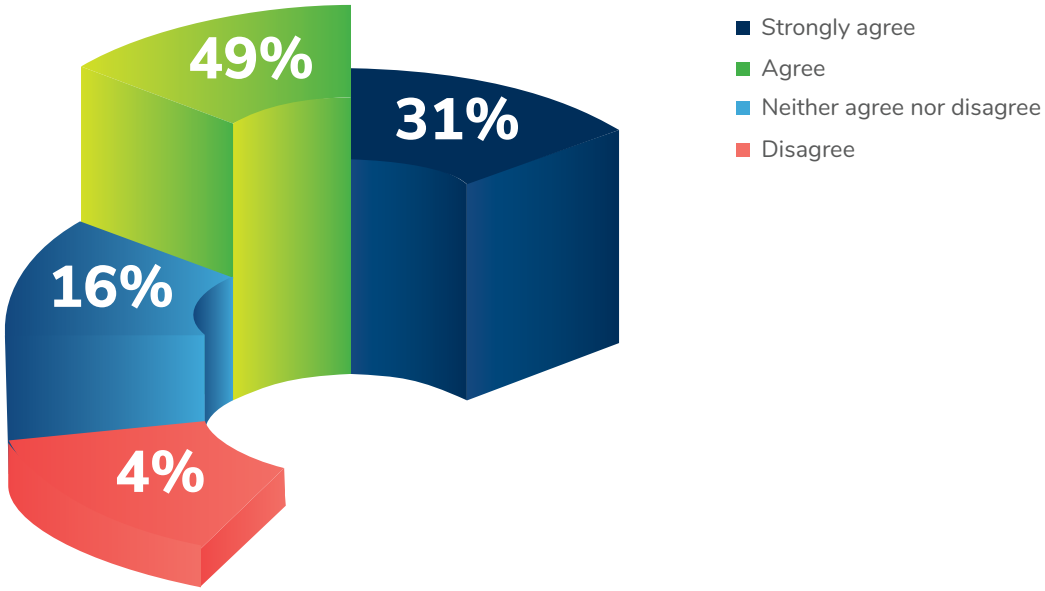
However, screening should go way beyond direct intermediaries, at least until regulation catches up with market practice and clear best practices and reputable intermediaries and institutions emerge who can be relied upon in this space. At least for now, screening and basic diligence should include reasonably attainable counterparties throughout the carbon credit value chain. That includes, for example, conducting diligence on the carbon registries themselves. Recent high-profile investigations, for example, have raised concerns around some of the more reputable carbon registries in the market. Companies need to watch the watchers to avoid getting caught up in headlines around improper credit usage or schemes.

Companies should also assess the broader ecosystem of project developers and any associated parties, including, but not limited to, identifiable landowners. The geographic locations of these projects often involve jurisdictions with limitations around transparency, rule of law, sovereign oversight capacity and, in some cases, are subject to high levels of public corruption. That creates perfect conditions for the use of carbon credit projects by organized criminal operations, including for bribery, money laundering and financial obfuscation schemes (for example, via opaque land registries and hidden beneficial ownership structures). Relatedly, companies should also better understand the nuances of jurisdictional risks and developments as evolving geopolitical or domestic political issues will likely impact some of these credits and result in their nullification. The Zimbabwe Government's recent takeover of the local carbon trading market is a prime example of how sovereign risk can materially impact project viability.

Project Accounting and Impact Risk

A further and frequently misunderstood risk factor concerns the underlying project accounting and determination of actual impacts on carbon emissions. Carbon credit projects are not created equal. In addition to having different credit-generating processes and mechanisms—including nature restoration, forestry, REDD+, energy efficiency, non-CO_2 gases, fuel switching and/or renewable energy—they also involve varying demand profiles and command different purchase price levels. Companies need to ensure that these projects address climate change by legitimately removing, reducing or avoiding emissions. That, after all, is the whole purpose of the credit regime. Fortunately, 80% of our survey respondents agree or strongly agree that they at least plan to take steps to verify that the purchased carbon credits are appropriately addressing climate change.

We Will Take Steps to Verify That the Purchase of Carbon Credits Are Addressing Climate Change and/or Promote the Growth of Renewable Energy



Until more regulation and clearly defined best practices and standards emerge, companies will need to rely on their own subject matter experts and/or credible and competent third parties to understand and scrutinize developers' claims about how emissions are reduced or removed as well as the mechanisms through which that reduction or removal occurred or will occur. That's especially true under current conditions, where the credit ecosystem and landscape continue to evolve in real time. Carbon credit accounting, for example, is based on the foundational concept of "additionality". As discussed earlier, at a theoretical level, additionality basically means that a credit project must demonstrate that it reduces or removes carbon from the atmosphere and would not have happened without the credits. That involves assessing and quantifying the underlying tons of CO_2e reduced or removed over a distinct period and, therefore, determining the permanence of the reductions and removals. In addition to having the right technical competence and expertise, determination of issues around additionality, quantification and permanence involves a degree of judgement and discretion.

Adding to the complexity, numerous potential standards, frameworks, principles, protocols (most importantly the Greenhouse Gas Protocol's project-level accounting) and other related technical issues have emerged to assist and provide methodological rigor around measuring, validating and verifying these components. These rules and standards are filtered through an ecosystem of registries and third-party organizations. While a "race to the top" around standards and methodologies should assist in theory, in practice there is still a lot of learning-by-doing involving a limited number of qualified subject matter experts, creating confusion and uncertainty in the market.

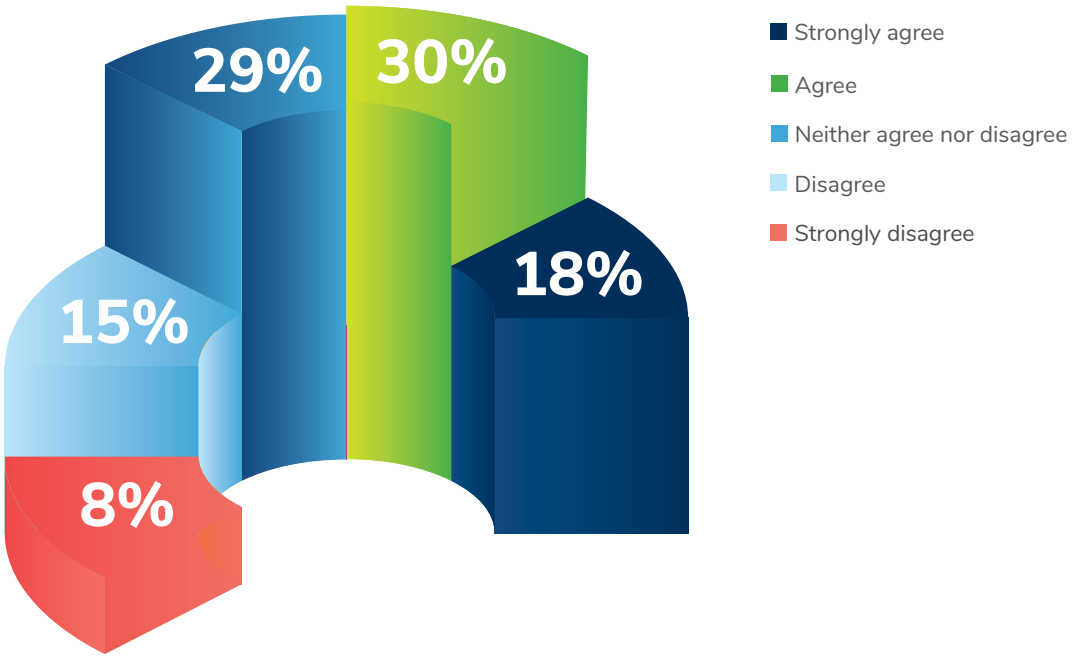
The confluence of technical, legal, regulatory and reputational issues surrounding carbon credit project accounting and development means that, until better regulatory oversight and bright-line standards emerge, companies will need to engage the right internal subject matter experts and knowledgeable third-party providers to assist with assessing the integrity of the underlying credits and the processes involved.

Disclosure and Communication Risk

Lastly, even for clearly legitimate carbon credits, there are important risks around their use. Companies must zealously commit to transparency and clarity in any related disclosures and communications with stakeholders about their climate programs and how carbon credits are being used. In particular, companies must ensure their climate-related and emissions reduction disclosures and communications do not risk misleading stakeholders, including investors, about their own climate-related performance, goals and targets, especially as it pertains to the use of credits in achieving carbon neutrality and any science-based net-zero targets.

Transparency and integrity around climate-related disclosures and communications starts with companies ensuring that their own emissions calculations and disclosures around GHG Scope 1, 2 and 3 emissions are aligned with existing best practices under the GHG Protocol and related quality-control standards and ensure that any assumptions, uncertainties, limitations and risks are duly disclosed.

Organizations That Agree They are Confident in Calculating Greenhouse Gas Emissions



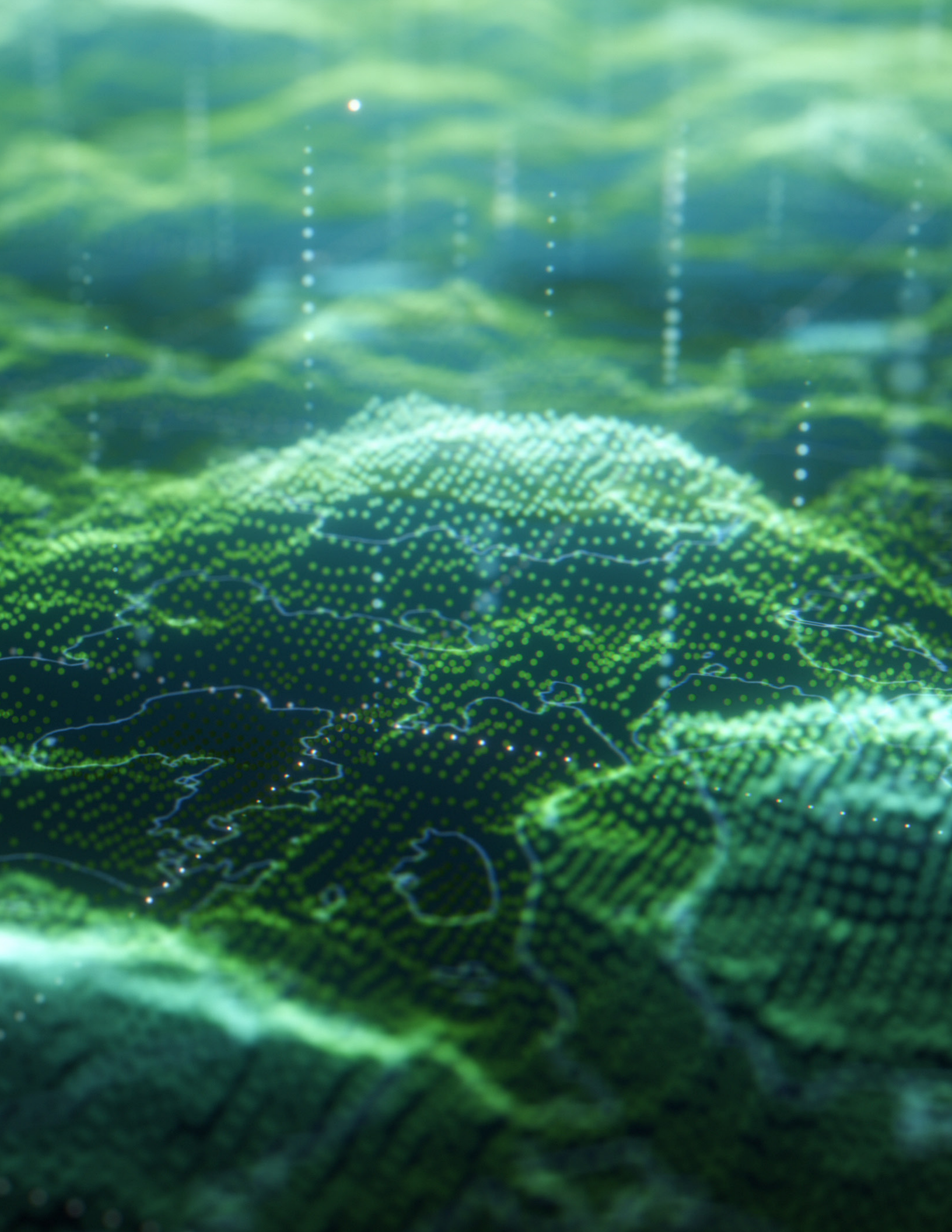
Despite the apparent confidence that a minority of firms have around their GHG calculations, most still struggle with data collection and are unfamiliar with the relevant standards and protocols and the underlying accounting calculations and mechanics. For example, while valuable as part of an overall emissions management program, carbon credits should never be used to directly reduce Scope 1, 2 or 3 emissions calculations and, relatedly, should not be used in calculating science-based climate targets (around net-zero calculations, for example). The most widely adopted and credible standard setter, the Science Based Targets initiative (SBTi), for example, makes it abundantly clear that credits should only be used to "neutralize" the impact of residual emissions after any targets have been achieved. Most importantly, companies must ensure that narratives and disclosures around emissions targets and carbon credits accurately portray exactly how they are being used, including their limitations. In the current environment, which is hyperfocused on greenwashing, even a modicum of misleading information or exaggeration on climate issues can raise major reputation and legal risks. As with all other ESG factors, zealous and rigorous transparency and integrity around disclosures and communications is of paramount importance. "Sunlight is the best disinfectant," as Supreme Court Justice Louis Brandeis once famously quipped over a century ago.

Proceed, but with Caution

Given all the uncertainties involved, companies may choose to refrain from voluntary carbon credits markets altogether. However, when used in the right way, carbon credits can arguably play a critical role in broader efforts to address climate change, including around neutrality goals and going beyond SBTi targets. In addition, better methodological guidance and standards from academic institutions and civil society organizations continue to evolve and advance in real time and carbon credit registries are making concerted efforts to address issues with the underlying project accounting and developments. Moreover, a cottage industry of solutions providers and standard setters is emerging to address many of the integrity-related issues raised above. Lastly, a slew of new regulatory standards and oversight mechanisms are set to transform climate-related and emissions disclosures and practices in the near future. In the meantime, and as this process unfolds, companies that choose to use carbon credits should look to their subject matter experts and service providers to navigate the uncertain terrain.

References:

https://www.theguardian.com/environment/2023/jan/18/revealed-forest-carbon-offsets-biggest-provider-worthless-verra-aoe
https://www.bloomberg.com/news/articles/2023-05-16/zimbabwe-plans-takeover-of-carbon-credit-trade-voids-past-deals



Challenges with ESG Reporting and Transparency

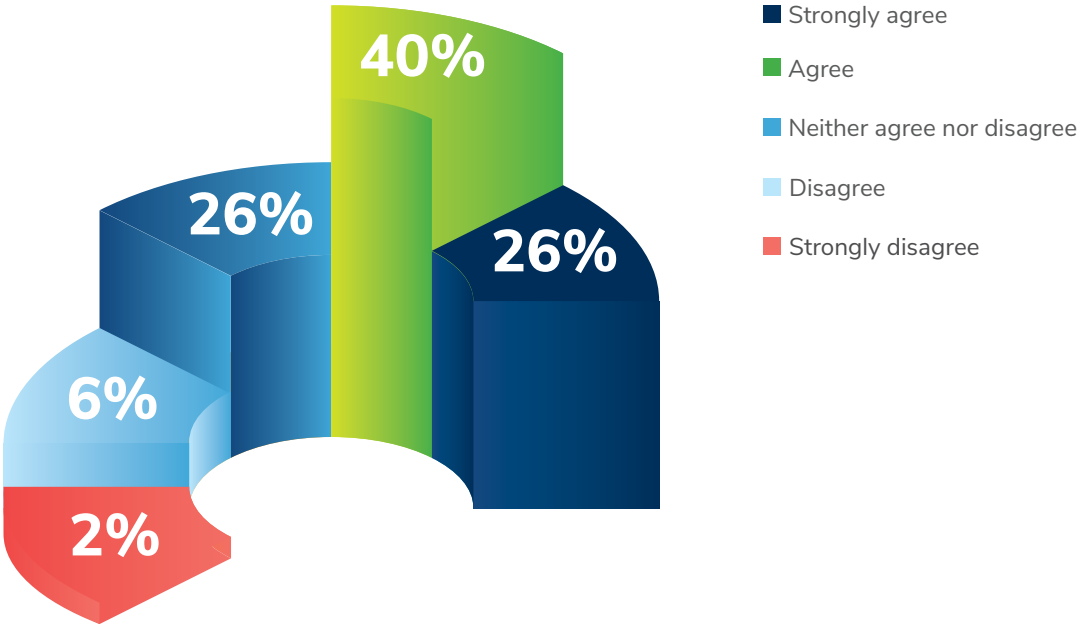
by Julianne Recine, Chris DeSa and Veronique Foulon

Firms must make a focused effort to explain and backstop their environmental, social and governance (ESG) initiatives and provide the steps they have taken or will need to take to achieve their goals. Telling the right ESG story in the current environment requires adequate and accurate disclosures both on performance on ESG-related accounting and activity metrics as well as the underlying methodologies, policies and procedures employed.

A best practice methodology includes conducting materiality assessments and measuring the amount of ESG risk and its impact on valuations and operations in both routine and stressful environments. A thorough materiality assessment is an introspective look into a firm that allows it to accurately form its ESG narrative and identify areas where it might improve or would like to further develop.

Most respondents in our survey appear confident that they are telling the right ESG narrative, either agreeing or strongly agreeing that their ESG/Sustainability story is an accurate representation of their activities and mission.

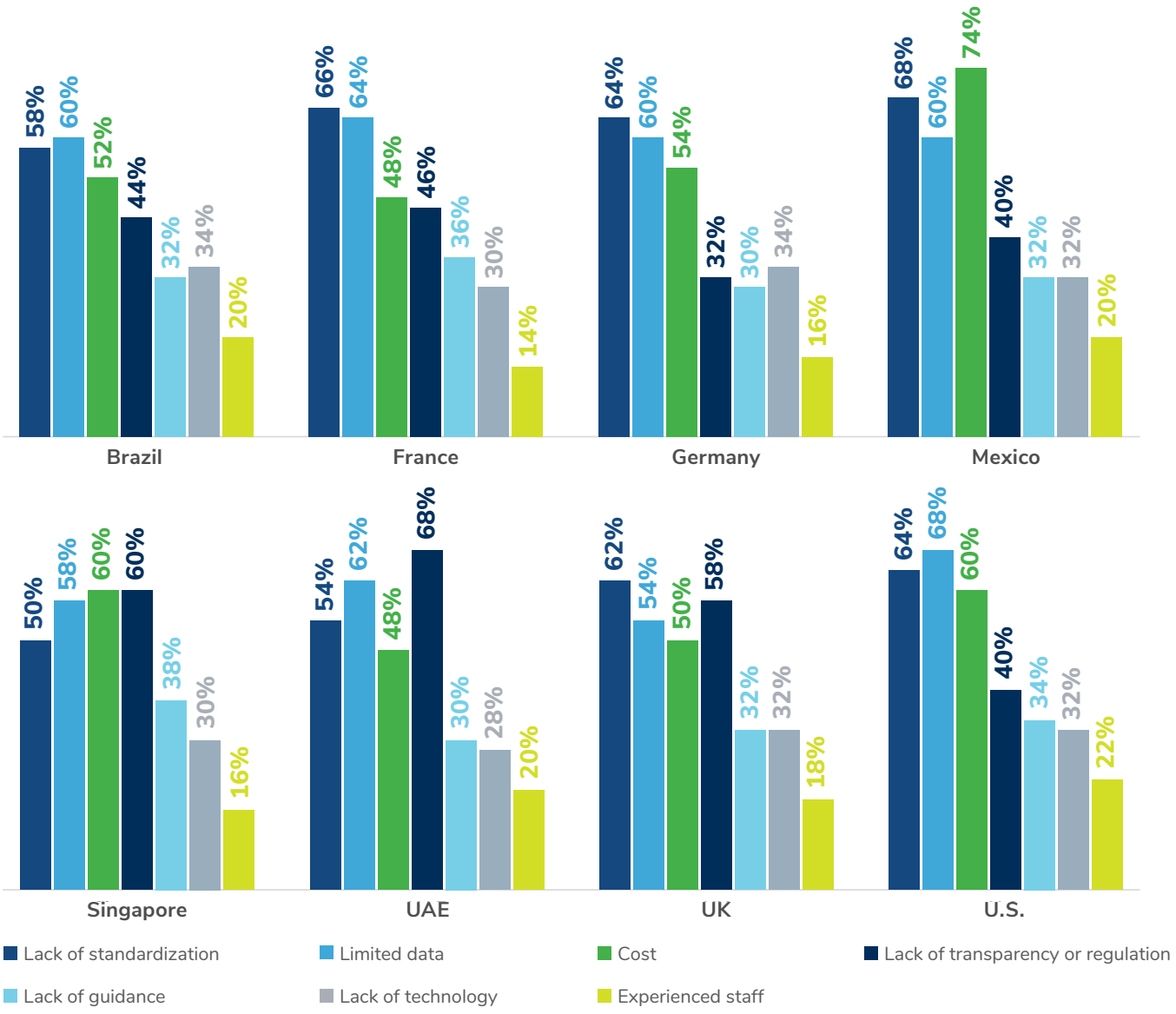
Organizations That are Confident Their ESG Story is an Accurate Representation of Their Company's Activities and Mission



Given the importance of ESG as a mechanism for disclosing and communicating companies' journeys and performance on sustainability issues, that should be a promising development. However, our survey also confirmed that most companies still feel challenged by the issues of standardization and data integrity that primarily relate to storytelling. That raises concerns that might belie the accuracy and adequacy of their ESG stories and whether they are focusing on the right factors.

Although survey respondents appear to feel confident in the accuracy of their ESG stories, they also state that they continue to face challenges and issues around methodological standardization and data collection, among other issues.

Across the Globe, Main ESG Challenges are Standardization, Data, Cost and Transparency



In other words, despite the arguably clearer picture in the current environment, firms continue to struggle with the underlying methodologies and data that enable adequate disclosures of the ESG story. Perhaps that is partly a function of legacy issues from the past decade's confusion and uncertainty. However, it may also be influenced by heightened temptations to meet "middle-of-the-pack" ESG disclosures and practices and avoid standing out, but while minimizing anticipated costs associated with complying and aligning with current norms. Companies may find it easier to embrace and disclose an unreflective slew of ESG factors and metrics with limited relevance, just to quickly appease certain internal and external stakeholders or align with competitors. However, that approach to ESG is an increasingly risky proposition; current improvements around standardization and heightened scrutiny also means the risks and potential consequences of improper ESG disclosures have also meaningfully increased. Technology is improving the ability to ask standardized questions and gather responses across a portfolio of assets. This enables the highlighting of outliers and risks

against a benchmarked view. Technology is not only enabling easier collection of data, but also the continuous assessment of indicators to allow for real-time status of risks.

Green Crimes

Environmental crimes are rarely spoken of within the scope of financial crimes, despite the effects being just as damaging as more commonly recognized forms such as fraud. Until recently, environmental crime was seen as a lower-risk activity for criminal networks, as governments across the world placed priority on tackling drugs, counterfeiting and human trafficking. Across many countries, light sanctions for environmental crimes alongside limited efforts to follow and remove the profits made participating in such activities a lucrative source of income for criminals. A few examples of green crimes that firms need to be aware of include illegal logging/trade, trafficking of protected species of animal and plant wildlife, smuggling precious metals and even waste management.

Currently, it is extremely difficult for firms to detect potential environmental crimes as there is no specific criteria of what to look out for or a blacklist of companies that are known to engage in illegal activities related to environmental crimes. However, there are key indicators that should ring alarm bells for firms about the legitimacy of a business and the potential for green crime activity. The main aspect to look out for are potential inconsistencies (for example, boards with no experience in the industry in question or companies that hold significantly higher profit margins than others within the sector). This requires an element of proactivity and good industry knowledge to apply in each individual case. Proper due diligence is the best way to identify potential risks associated with green crimes or other ESG-related activity.

The Consequences of Getting ESG Wrong

At a minimum, firms that fail to adopt proper ESG practices are likely to misallocate resources and focus on factors of less importance, undermining the point of ESG and its focus on real issues, including the enterprise's social license to operate, the use of common capitals (or natural public resources) and the negative externalities created by its operations.

Firms that do not adopt current recommendations substantially increase the likelihood of greenwashing, fraud and abuse, either knowingly or unknowingly. Failing to adopt best practices and proper policies and procedures creates conditions for unintentional misstatements and errors. Failure to do so can initiate problematic situations involving outright fraud and criminal malfeasance, both by the organization itself and opportunistic third parties. For company insiders, incentives are extremely high to make statements that suggest excellence in ESG metrics or activities around the level of adoption of policies and procedures.

The Overlooked G in ESG

The governance pillar (G) is sometimes overlooked in the context of ESG programs when compared to its environmental (E) and social (S) counterparts, yet it is the fundamental basis of any ESG compliance program and the initial path to develop and implement any ESG, impact or sustainable investment strategies and priorities for a company. This means defensible, thorough and efficient controls both on the source of data and its analysis. Transparency and discipline also allow stakeholders to understand and balance the business decisions and trade-offs associated with a comprehensive ESG program. It is, in short, the common thread that weaves together all ESG efforts.

Governance is an essential component of managing ESG risks well. The G pillar includes factors such as independence of the board, shareholder rights, executive compensation, risk and control procedures, operational due diligence, anti-competitive practices, business ethics, fraud and respect for the law and regulations. Instances of weak governance invite shareholder litigation and regulatory action.

ESG and Data Standardization

By 2021, 86% of S&P 500 firms regularly issued some kind of ESG-related report, up from 35% of publicly traded companies in 2010, according to the Harvard Business School. There is no one-size-fits-all solution to a company's ESG program and although there has been some regulatory guidance and stakeholder pressure, standardization is still lacking. Certain jurisdictions will have different views of ESG and how critical it is to their business' success.

Regulatory requirements and client, investor and consumer expectations will influence the ESG-related data that is collected. With a variety of ESG reporting frameworks and standards, many organizations are faced with the challenges of aggregating data from their suppliers or portfolio companies or even at their own corporate level. Adding to confusion is the lack of or limited data that companies have access to or are able to aggregate for their own reporting purposes. There is also a lack of verifiable and consistent data. Most firms have limited in-house resources, which may lead to improper and/or inadequate internal controls of their ESG programs. Solutions that bring ESG expertise in-house can be costly. And as with any regulatory framework, it may take time to bring staff up to speed with ESG regulation and reporting expectations. Technology solutions can be beneficial in helping companies standardize their ESG data aggregation, but many providers tend to simply aggregate data without providing meaningful reporting and benchmarking.

According to our survey results, 61% of respondents cited a lack of standardization as a key ESG challenge and 61% cited limited data as their key challenge. Firms concerned about litigation and enforcement risk, particularly in jurisdictions where the regulatory framework is not clear, should ensure that any limitations and weaknesses in data and disclosures are fully understood and disclosed, including any applicable data gaps and methodological limitations. In-house or external counsel should review any related disclosures prior to their release to ensure alignment with applicable local disclosure rules and regulations.

ESG Risks and Rewards

As discussed above, transparency is often an effective balm for organizations working with murky data. Delivering on stakeholder expectations while working with uncertain data can be difficult, but truthfulness about the uncertainty, along with a strategy to improve it, is a better outcome than being accused of greenwashing.

Many global regulators are focused on ensuring that firms are adhering to their ESG commitments by providing proper disclosure and reporting to investors. In short, a firm can't simply state its commitment to ESG without being prepared to provide evidence of adhering to those commitments. Documented compliance programs, data and an understanding of the data's lineage, and transparency about the data's limits will be required to respond to client and regulator inquiries.

Firms that have successful ESG policies face the lowest risk and are dispassionately introspective while assessing themselves. They take due diligence, internal education and risk management seriously.

Harvard Business School "Are Companies Actually Greener-or Are They All Talk?" by Rachel Layne
Harvard Business School article

The Path Forward

In a global environment of evolving economic pressures, geopolitical tensions and cutting-edge technological advancements, the significance of an adaptive, tech-driven strategy in combating financial crime is more critical than ever. Our findings spotlight the importance of technological adoption in anti-money laundering efforts, alongside the complexities of customer onboarding and monitoring.

The recurrent theme of balancing transparency and privacy, notably in beneficial ownership, calls for cautious navigation. Likewise, in environmental, social and governance reporting, businesses must align with evolving standards to avoid the pitfalls of greenwashing and fraud.

The dynamic sanctions landscape and the burgeoning world of cryptocurrencies present unique challenges. Companies must leverage technology to ensure compliance and mitigate risk. The anticipated surge in anti-bribery and corruption enforcement actions underscores the necessity of a proactive approach.

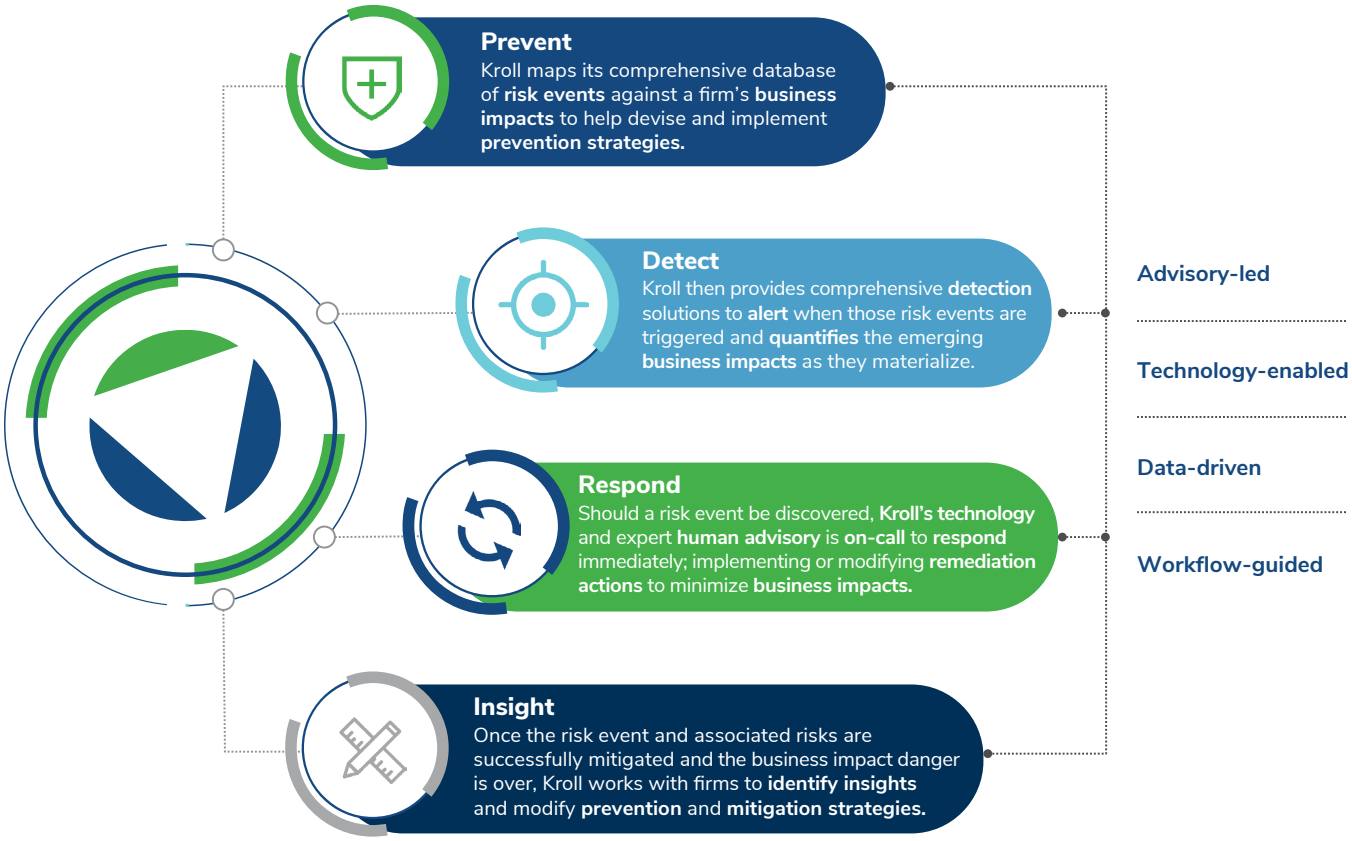
As we look towards the future, the convergence of technology, geopolitics and financial crime brings an intricate web of risks but also opportunities. Compliance officers, regulators and risk analysts play a crucial role in this complex environment, highlighting the importance of continuous learning, adaptation and a firm commitment to ethical conduct and good governance.

In the face of this dynamically evolving landscape, the role of the compliance function remains more crucial than ever. It is our sincere hope that 2023 serves as a turning point, a year when we not only recognize the challenges posed by financial crimes but also identify and implement impactful strategies to combat them. Harnessing technology advancements, strengthening governance and fostering transparency will be key to our collective success in this ongoing fight against financial crime.

We extend our gratitude to all those involved in this endeavor, from our survey participants to the passionate professionals committed to reducing financial crime. Your insights, contributions and commitment provide a vital roadmap in this time of uncertainty. Kroll remains ready to collaborate with you, lending expertise and assistance to boost your financial crime compliance and to meet your program objectives. As we move forward, let's strive for a future marked by resilience, responsibility and progress in our collective fight against financial crime.

Kroll's Integrated Risk Intelligence Solution

The integration of risk, compliance, audit, internal controls and incident management workflows onto a single platform is essential to the creation of an efficient and effective program. Kroll's integrated risk intelligence solutions leverage our unique insights, data and technology to help clients stay ahead of the complex and ever-evolving corporate risk landscape. Preventing, detecting and responding to risk requires a proven combination of investigative experience, cutting-edge technologies, deep subject matter expertise, local and global knowledge and data-driven insights.



Fraud and Financial Crime Capabilities

Successfully identifying and remediating these forms of malfeasance often requires a multipronged approach that cuts across specializations and geographies. Our global team of former regulatory and compliance officials, investigators, cyber experts, data analysts and forensic accountants draw upon extensive experience, resources and technologies, to help identify and mitigate the risk of fraud, corruption and money laundering before they occur.

- **Anti-Money Laundering (AML):** Our AML solutions are designed to help minimize the risks associated with money laundering and other illicit activities and to ensure compliance through the development and management of ongoing compliance programs and processes.

- **Cryptocurrency Compliance, Risk and Investigation:** We assist clients in need of regulatory guidance, investigations and asset recovery. Our work enables clients to manage risks, enhance AML programs customized for digital asset products, and trace and recover funds involving digital assets.

- **Anti-Bribery and Corruption (ABC):** We help clients prevent, detect and respond to fraud and corruption risks. Our international network of offices and contacts gives us the local knowledge and capabilities in jurisdictions around the world, enabling us to uncover fraud and corruption in emerging or frontier regions that can be challenging for outsiders to navigate.

- **Business Email Compromise (BEC):** From misdirected payments to the compromise of sensitive data or unauthorized access to the wider network environment, we help our clients through any challenges stemming from a BEC attack. We help investigate and remediate compromises, prepare your organization against a BEC attack, perform email and cloud security assessments to help harden mailboxes, assist with cloud system configuration and monitoring and conduct simulated phishing attacks to help educate your staff.

- **Environmental, Social and Governance (ESG):** Our ESG advisory and technology solutions help clients comply with ESG regulation and discourse reporting, develop ESG policies, reduce risk, embed ESG across governance and areas of business and deliver sustainable value and growth.

- **Sanctions:** We provide comprehensive support for clients to detect, mitigate and remediate sanctions compliance risk through our sanctions screening solutions, program advisory and investigative capabilities. Our multidisciplinary approach helps clients anticipate ever-evolving regulatory demands.

- **Insider Threat Investigations:** Our insider threat investigators combine world-class computer forensic expertise with traditional investigative methodology to retrace the behavior of people who may have had access to protected or proprietary data and might be looking to take advantage for financial gain. Additionally, our insider threat investigators have experience handling bribery and corruption investigations, delivering comprehensive, unbiased and confidential reports.

- **Managed Detection and Response (MDR):** Kroll Responder, our MDR solution, merges frontline threat intelligence with incident response experience from thousands of investigations we manage every year to provide 24x7 detection and response. We utilize rich telemetry from endpoints, network, cloud and Software-as-a-Service providers to deliver enhanced visibility and rapidly shut down cyber threats across your digital estate.

KROLL

Across 34 countries and territories

The Americas

Atlanta
Austin
Bermuda
Bogota
Boston
Buenos Aires
Chicago
Dallas
Diamond Bar
Ellensburg
Houston
Los Angeles
Mexico City
Miami
Minneapolis
Morristown
Nashville
New York
Philadelphia
Richardson
San Francisco
Sao Paulo
Seattle
Secaucus
Silicon Valley
Toronto
Washington DC
Waterbury

Caribbean

British Virgin Islands
Cayman Islands

Europe, Middle East and Africa

Abu Dhabi
Agrate Brianza
Amsterdam
Barcelona
Berlin
Bilbao
Birmingham
Brussels
Channel Islands
Dubai
Dublin
Frankfurt
Gibraltar
Guernsey
Johannesburg
Lisbon
London
Luxembourg
Madrid
Manchester
Milano
Munich
Padua
Paris
Pesaro
Riyadh
Rome
Tel Aviv
Turin
Zurich

Asia Pacific

Beijing
Guangzhou
Hanoi
Hong Kong
Hyderabad
Jakarta
Kuala Lumpur
Manila
Mumbai
New Delhi
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo

KROLL

About Kroll

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.