Financial Crime Predictions for 2023

cable

Cable is the complete effectiveness testing platform for financial crime compliance and oversight

Anything less than full monitoring of controls leaves room for error - finally you can do away with manual dip sampling. Cable provides automated evidence of your compliance, risk management and effectiveness, allowing you to:

- **save money by eliminating expensive remediation projects,**
- **reduce the risk of regulatory fines,**
- **save time by automating reporting,**
- **improve stakeholder communication, and**
- **scale compliantly and with confidence.**

Why manually test 100 accounts when you can automatically monitor 100%?

Introduction

With 2022 drawing to a close, what will the 2023 financial crime landscape look like?

We spoke with industry experts at Alloy, Alloy Labs, Fintech Business Weekly, Griffin, and Treasury Prime to learn what next year holds in store for financial crime regulation, compliance trends, compliance programs, and enforcement.

Looking Ahead At: Regulation

Bank-fintech relationships are in the spotlight

The Banking-as-a-Service landscape is on the forefront of regulators' minds. The last few months have seen a flurry of activity and conversation about bank-fintech relationships, with US regulators at the OCC and CFPB in particular addressing risks in these relationships. Many deficiencies have centered on BSA/AML compliance and inadequate systems and personnel for third-party relationships.

Next year should see this trend continue. Both in the US and the UK, standards for these arrangements have not been fully set out. A growing number of regulators are expected to look at these relationships from financial crime compliance and other perspectives. Further regulatory activity will likely bring additional clarity and expectations around partner banks' responsibilities and how they should meet their compliance obligations.

"It's reasonable to think there will be some form of regulation or guidance in 2023 that provides regulatory agencies more direct authority, control, or insight into the 'supply chain' of banking products and services and banks' partners, whether fintechs or embedded finance companies, and clarifies what expectations apply to them."

Sheetal Parikh
Associate General Counsel, VP of Compliance at Treasury Prime

All of these developments will likely affect how banks conduct oversight, collaboration, and continuous monitoring of their fintech partners, as well as their downstream service providers.

Our experts thought the prospect of greater regulatory clarity around bank-fintech relationships and the proper equilibrium amongst all the parties involved is a positive trend for compliance leaders going into next year.

For example, our experts agreed the OCC's new Office of Financial Technology – while it remains to be seen exactly how the office functions – is a good indicator of the regulator's intent to devote attention to bank-fintech relationships, invest resources in understanding the ecosystem, and figure out how to make these innovative arrangements work.

The greatest impact of these new regulations may fall on institutions just entering the BaaS space, as they lack an appreciation of the heavy lift required to build the necessary compliance infrastructure. Existing BaaS and partner bank models already adhering to best practices for fintech oversight will be able to adjust more easily.

More crypto rules to come forth

Following the FTX scandal and the past year's volatility in the crypto markets, our experts agreed crypto will be heavily scrutinized by regulators. Compliance leaders can expect a continuation of previous years' trends, with regulators strengthening and increasing the number of regulatory requirements for all parties in the crypto value chain. From a financial crime perspective, regulatory concerns likely will continue to revolve around crypto's lack of transparency and the difficulties in detecting suspicious crypto activities.

Rules imposing some form of limits on crypto exchanges would not be unexpected next year, though that would still be just a limited first step. Additionally, one of the difficulties with crypto regulation is determining which regulator has enforcement authority – compliance leaders may see greater clarity on that question over the course of next year. Finally, compliance leaders might also keep an eye on CBDC regulation to see how developments there may affect the crypto landscape.

Increasing access to beneficial ownership information

Our experts also noted that next year should bring several notable developments in beneficial ownership. In the UK, anticipated reforms to the role of the UK companies registry, Companies House, will likely offer compliance teams a more robust data set to identify and verify beneficial owners. In the US, compliance leaders should focus on the continued implementation of the Corporate Transparency Act, which will impact about 33 million businesses that will have to file beneficial ownership information directly with FinCEN.

Sanctions developments will demand close attention

This past year saw unprecedented sanctions activity following the Russian invasion of Ukraine. While further regulatory developments depend heavily on the course of global events, compliance leaders should be prepared for increased regulatory focus on expanding sanctions regulations and oversight expectations, along with more unified international agreements to fight financial crime by locating assets across borders.

Looking Ahead At: Compliance Trends

Compliance teams will need to do more with less

With increasing compliance fines and rapidly changing regulations, compliance teams would typically be looking to expand headcount.

However, going into next year, the economic downturn will cause many institutions to cut expenses where possible. While compliance teams generally will be one of the last functions to face cuts, compliance leaders should expect economic conditions to force their teams to become more efficient and embrace new methods or tools.

According to our experts, this means that next year will bring increased pressure on compliance teams to automate processes and become more cost-effective with existing resources.

Teams that rely heavily on manual processes won't be able to keep up with business needs easily, so they will have to seek out technology solutions, or otherwise institutions will have to limit their customer numbers or activities.

"The reality is that banks need to automate any manual processes that can be outsourced to a machine, and use their personnel instead for ever-increasing compliance challenges. Trying to manage expenses without adding more personnel will lead to people who are stretched too thin or corners that need to be cut in order to keep up."

Jason Henrichs
CEO at Alloy Labs

"In recent years, founders and early stage companies are taking compliance much more seriously. If you're starting a tech company, it's part of the ethos that you need to buy the best compliance solution and hire experts, instead of trying to build a solution on your own. It's become de facto to get live and I don't think it's up for debate anymore."

Laura Spiekerman
Co-Founder & CRO at Alloy

Compliance will be a competitive advantage

In the current regulatory environment, more and more banks and their partners view compliance as a competitive differentiator or advantage.

The most successful institutions already embrace this perspective, but compliance leaders across the industry will need to come together to set standards for collective emerging compliance issues, like identity verification, third party due diligence, and information exchanges. This will bring a more unified sense of appropriate risk management practices to banks, fintechs, and other regulated firms.

Our experts said regulators' message has been clear for compliance leaders - your business cannot scale without dedication to compliance.

Next year should continue the trend of more leaders at the highest levels of organizations becoming actively involved in creating a broad compliance culture, rather than limiting compliance to certain functions.

Looking Ahead At: Compliance Programs

What financial crime risks will compliance leaders face in 2023?

Fraud and identity theft are on the rise

With the cost of living crisis, our experts agreed fraud is expected to rise next year and is a major concern for institutions. Criminal actors can be incredibly sophisticated in finding ways to exploit the economic downturn. Compliance teams should watch for increased organized criminal activity or greater use of money mules.

Some institutions also report seeing upticks in targeted fraud involving low-value, frequent transactions – compliance teams should ensure they are adequately monitoring money movement in and out of accounts to combat this fraud.

Sanctions landscape will remain fraught with risks

The shifting sanctions landscape will also continue to pose significant risks. While list-based sanctions may seem straightforward, the rapid proliferation of sanctions means that implementing appropriate, recurring screening in an operationally feasible way should be top of mind for compliance leaders.

Additionally, after observing the massive fallout from the sanctions on Russia, some institutions are scenario planning for their potential sanctions exposure to other commercially significant jurisdictions, namely China.

In the medium to long-term time horizon, compliance leaders should also note the development of alternative payment networks or schemes in China and other jurisdictions to avoid dependence on the US, which will increase the level of sanctions risk for everyone globally.

How are compliance programs being strengthened for 2023?

Demonstrating compliance program effectiveness through automation

Compliance leaders should expect regulators to continue to demand that institutions not only have policies and show best efforts at compliance, but demonstrate their compliance programs are actually effective, with proactive reporting of any deficiencies.

These pressures will be particularly relevant for compliance leaders in the partner bank context, as increased oversight expectations on banks will trickle down to banks' information demands from their partners.

Compliance leaders may struggle with the operational burden to uplift their ability to measure and demonstrate compliance program effectiveness, but it is increasingly critical for compliance leaders to get this right.

"We are seeing increasing numbers of fintechs, BaaS platforms, and partner banks trying to make transparency and read access in bank-fintech relationships more real-time and holistic, with focus not only on compliance policies, but also on the actual entities and the decisions that were made."

Laura Spiekerman
Co-Founder & CRO at Alloy

Our experts agreed that automated technology will be a significant add-value to these efforts by making it easier for companies to demonstrate that their controls have been operating correctly without creating additional work for their teams.

Compliance leaders should expect automation to be pivotal next year for compliance programs at institutions of all sizes, not just big banks – and, in particular, for banks in the BaaS space, automation will be absolutely essential to successfully manage those programs.

"The only realistic way to make BaaS programs scalable is to automate tasks that are typically manual. Option one is to hire dozens of compliance staff, but this will eat into margins and may not be a realistic option. Option two is to automate and empower the staff you have to scale. The opportunity for better automation is the only realistic way forward."

Jason Mikula
Founder at Fintech Business Weekly

Improving identity verification technology and processes

Reducing onboarding friction for identity verification through smarter tools and better processes will also be a big area of emphasis for compliance programs.

Compliance teams are focusing on increasing collaboration with other departments, like vulnerable customer teams, to better identify risks and avoid data silos.

Compliance leaders should also look for opportunities to collaborate around identity verification processes across the industry, as standardizing approaches helps raise the bar for everyone together.

Technology developments in compliance teams' use of data will offer significant improvements to identity verification processes.

Compliance leaders are looking for tools to increase the availability of data either across fraud and AML teams in a single organization or across organizations, or that even improve the use of open source data to identify threats. Institutions are also building better data models to incorporate all relevant data endpoints for identifying potential risks.

More compliance leaders will embrace or experiment with machine learning and adaptive algorithms as exciting new tools that enable far more sophisticated targeting of fraud, money laundering and financial crime typologies.

"One of the big causes of remediation projects is KYC controls that have not been kept up to date. Many banks are identifying that dynamic reviews – which are triggered by risks and leverage technology and data in an efficient manner – are a very good way of reducing their potential exposure."

Alex Nash
MLRO at Griffin

Looking Ahead At: Enforcement

Enforcement likely to be more active as regulators work through past issues

Regulators are increasing staffing and investing in other needed resources, but they will also be stretched thin with the amount of regulation that needs to be done next year, from new crypto requirements to beneficial ownership rules.

"We saw significant fraud in 2021 and 2022, with huge amounts tied to PPP and other programs. Going into next year, we are likely to see some regulatory fallout from that in the form of enforcement actions and committee hearings."

Jason Mikula
Founder at Fintech Business Weekly

As a result, regulatory enforcement will likely be more active, but actions may be more likely to involve penalties meant by regulators to set examples for the market or "clean up" past activities that are no longer tolerated.

It would not be surprising to see further enforcement actions next year involving bank-fintech relationships. Additionally, events of the past years may give rise to enforcement actions, such as actions for PPP fraud or further regulatory fallout from FTX.

Finally, sanctions are likely to continue to be a source of enforcement activity as regulators work their way through violations that have arisen in the past year.

Ineffective compliance programs invite potential actions

Regulators' tone has shifted from offering softer recommendations about compliance programs to expecting that institutions adhere to best practices. Enforcement actions in the next year will likely see regulators focusing on whether firms have implemented appropriate risk management and oversight systems as a root cause for any control weaknesses.

Compliance leaders should focus on whether testing has been enforced on all of their AML requirements – if issues remain unnoticed, the scale of remediation projects can quickly become all-consuming and potential penalties skyrocket, making automated testing all the more important for compliance teams.

Conclusion

As we head into the next year, the pace of regulatory change is only increasing.

It's essential for institutions and compliance leaders to have robust and trustworthy horizon scanning programs to see what is coming and obtain the tools and technology needed to equip their teams to succeed.

Looking to automate your financial crime oversight and assurance

Contact us here to learn more about Cable or to see our platform in action

cable

cable.tech