SymphonyAI

Sanctions in focus – how new AI tech is adding business value

Featuring expert insights from SymphonyAI and Kharon

Introduction

As global banking increasingly operates under the shadow of complex and ever-changing sanctions, financial institutions face mounting challenges in ensuring adherence to international regulations. Navigating this intricate landscape can often seem daunting, especially for organizations striving to maintain both compliance and a competitive edge.

This guide offers a deep dive into how cutting-edge AI technologies are revolutionizing the way businesses manage and respond to sanctions. By automating routine tasks, enhancing due diligence, and providing real-time insights, AI not only helps to mitigate risk but also drives operational efficiency and strategic decision-making. Through a series of expert-driven questions and answers, we explore the transformative potential of AI in compliance, highlight current trends, and provide actionable insights for leveraging these technologies to add tangible business value.

Whether you are a compliance officer, a business leader, or a technology enthusiast, this guide will equip you with the knowledge and tools necessary to harness the power of AI in navigating the complex world of sanctions.
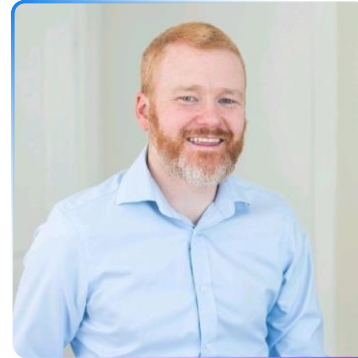
Join us as we delve into the future of compliance and discover how AI is reshaping financial institutions and the corporate landscape in profound and exciting ways.

Roundtable panelists

Charmian Simmons

Financial Crime and Compliance Expert, SymphonyAI

Enda Shirley

Head of Compliance, SymphonyAI

Ben Princen

Sanctions Product Manager, SymphonyAI

Howard Mendelsohn

Chief Client Officer, Kharon

1   What are the key developments and trends in sanctions compliance and enforcement over the past 12 months? Do you see this changing in 2024?

Simmons

New sanctions designations, sanctions anti-circumvention, and sanctions evasion top the key trends in the past 12 months. The European Union (EU) and the US released substantial named individuals and entities to sanctioned lists in the wake of the Russia-Ukraine situation. The EU's twelfth and thirteenth sanctions packages introduced new trade measures for anti-circumvention that extend across the globe, including limiting military tech for warfare, while the UK published its first sanctions strategy in early 2024. These aim to weaken Russia's war efforts against Ukraine, address global threats, and enhance sanctions implementation and enforcement.

In terms of enforcement, we saw greater steps taken to enforce economic, sectoral, and trade sanctions. For example, there was the enhanced partnership between the US Department of the Treasury's Office of Foreign Assets Control (OFAC) and the UK's Office of Financial Sanctions Implementation (OFSI), which issued several joint industry guidance and engagements, and more recently unveiled sanctions against Chinese state-backed hackers over alleged 'malicious' attacks regarding upcoming elections.

We can expect to see these trends continue in 2024.

Shirley

Organized crime group the Kinahan cartel offers a pertinent example of the evolving landscape of sanctions compliance and enforcement. The US OFAC (April 2022) designated the cartel and several of its key members and three associated businesses under Executive Order 13581, aimed at "Blocking Property of Transnational Criminal Organizations". This was a collaborative effort involving OFAC, the Drug Enforcement Administration, the US Department of State, US Customs and Border Protection, Ireland's national police force, the UK's National Crime Agency, and the EU Agency for Law Enforcement Cooperation.

The sanctions against the Kinahan cartel – targeting an organized crime group and its leadership for their roles in international narcotics trafficking and money laundering – highlight a significant trend in sanctions enforcement: the global reach of US sanctions authority and the increasing collaboration among international law enforcement and regulatory bodies to combat transnational criminal organizations.

Princen

The Russia sanctions are still prevalent and unlikely to change soon. More effort will be required to enforce even more sanctions against Russian individuals and entities with loopholes investigated more closely.

We are also seeing more aggressive enforcement of sanction regulations, with the regulators stepping up their game. Secondary sanctions make the name-screening landscape even more complex, alongside cryptocurrencies. New technologies are being developed and used to improve screening, but other new technologies are being used to avoid it. We expect that technology will have a big impact on sanctions in the next few years.

36%

Increase in sanctions (4,521) against Russia between 1st January and 31st December 2023.

Source: Sanctions lists in Australia, Canada, EU, France, Russia, Switzerland, UK, UN, and US, covering 1st January-31st December 2023. Excludes embargo-type sanctions programs which target an entire industry or country.

Mendelsohn

Export controls have risen to a level alongside sanctions as a top national security matter. For over a year, The Five Eyes, EU, and Japan have issued a largely consistent body of guidance calling on financial institutions to take steps to identify and report on both Russian sanctions and export control evasion. At the forefront of this effort is the Common High Priority Items List, which lays out 50 goods classified by Harmonized System (HS) Codes for risk of diversion.

Additionally, an advisory from OFAC accompanying EO 14114 issued late last year calls on industry to use "open-source information and past transactional activity to inform due diligence and to conduct proactive investigations into possible sanctions and export control evasion." This guidance acknowledges that there is an opportunity for banks to spot evasion within their existing transaction base. Effective detection requires using the right tools and open-source intelligence to isolate high-risk activity that goes unnoticed in traditional screening and monitoring processes.

Enforcement authorities have targeted small cells illegally shipping sensitive technology to restricted parties and jurisdictions – but there has yet to be a penalty on a corporate entity related to activity post the February 2022 invasion.

Overall, last year featured increased emphasis from the public sector calling on industry to be more proactive and innovative in detecting and reporting exposure to diversion, particularly with respect to Russia. For leading risk managers, this year will be an opportunity to showcase best practices and effectiveness.

2   Are sanctions complexities still a pressing issue facing financial institutions and corporates this year? What can they do to ease the burden?

Simmons

Absolutely. Sanctions complexities continue to be an ongoing issue due to the intricate and multifaceted landscape of international sanctions, whether it's the expanded scope of sanctions imposed at a country level, such as those by the EU or US, or the 40+ government elections taking place in 2024 that will change designations. The complexities also include trade and payments to third-country facilitators for warfare in Ukraine, Gaza, Israel, etc., and the changing payments landscape as message standards/frameworks/data fields change to accelerate faster payments. Also, there are the 'gray' aspects of sanctions screening, monitoring continuing to grow, and alert investigations requiring greater attention and time.

Financial institutions can deal with these sanctions complexities by moving to advanced sanctions software solutions that scale to handle high volumes, offer high match accuracy upfront, and streamline the investigation process to improve efficiency and effectiveness. SymphonyAI's [SensaAI for Sanctions](#) and [Sensa Investigation Hub](#) are such examples that handle this with ease.

Shirley

In 2024, navigating the intricacies of sanctions compliance remains a formidable challenge for financial institutions and corporations. The dynamic landscape of international sanctions, spotlighting regions such as Russia and China along with groups linked to terrorism, coupled with rapid technological progress, requires a more nuanced and advanced compliance strategy. This complex environment demands continuous adaptation and sophisticated solutions to stay aligned with global compliance mandates.

> " Navigating the intricacies of sanctions compliance remains a formidable challenge for financial institutions and corporations.
>
> **– Enda Shirley**

Princen

We see increasing pressure from regulators to enforce sanctions and to go beyond what is strictly necessary. The number of designations is still rising fast and increases both technology and investigator costs, with a larger workforce required to deal with the surge in name screening hits. Due to more complex attempts to avoid detection, investigations also take longer.

False positives have always been the biggest problem in sanctions screening, and this is still the case. What we have seen, though, is that a lot of these false positives, both in transaction and name screening, can be dealt with in an automated manner. The way to deal with these cases depends on financial institutions' risk appetite and the regulatory landscape, but we definitely see more acceptance of AI-driven solutions. While still early days, AI is finally becoming capable of dealing with name screening scenarios.

Right now, there is a definite advantage to implementing automated alert-handling solutions for all financial institutions.

Mendelsohn

A critical challenge this year will be to improve detection and effectiveness in countering evasion. Reliance on legacy controls focused on government list screening and adverse media monitoring will not be effective.

To ease the burden of false positives and noise, institutions using high-quality risk intelligence will demonstrate both efficiency and effectiveness on some of the highest national security matters, whether on Russia, Iran, or dealing with forced labor from China.

> " AI is finally becoming capable of dealing with name screening scenarios.
>
> **– Ben Princen**

3 What steps can financial institutions and corporations take to build a complete, accurate picture of a potential customer or business partner as it relates to sanctions?

Simmons

Having a holistic view of a potential or existing customer (individual or business entity) that is dynamic and, therefore, up to date supports faster decision-making when it comes to the screening and monitoring of sanctions. Shell companies, unusual ownership structures, common names and spelling, known relationships to other entities, etc., can easily obscure the true origins of a customer, how well you know them and their typical operating behavior, and the speed at which potential sanctions hits can be resolved.

The right type of technology and data-driven results for perpetual profiles and risk scores, such as AI risk score, dynamic risk scoring, and transaction behavioral patterns automatically informing risk scores, have proven to be highly effective in deciding proceedings and outcomes in improving the accuracy of matching and in resolving potential designation list matches.

Shirley

Start by ensuring the foundational elements of the compliance program, as it relates to name screening, are in place. This means ensuring rich and accurate data is captured against an organization's direct customer base. Provisions must be in place for all existing customers to be screened against new suspicious individuals (those added to lists) on a daily, if not more regular, basis and for all new customers to be screened against all suspicious individuals.

With the foundations in place, sanction programs should extend their reach from their primary customer base to their associations, uncovering connections to sanction at one or even many degrees of separation away. This should harness the growing available external sources of data and build out a clearer connected picture of risk for the organization.

Princen

Name screening is just the starting point. Often, red flags are not strictly confined to a name hit but are also a strong indication that something needs to be investigated further, with name screening expanding into screening of connected parties, and different categories than just sanctions. We have seen a strong rise in interest in adverse media screening and location screening, for example.

A risk-based approach is essential to be able to target the correct hits. A financial institution must implement a screening system that is in line with their risk appetite.

Mendelsohn

The baseline for effective KYC at account opening includes (but is not limited to) collecting data on owners, beneficial owners, guarantors, and senior management, as well as developing an understanding of their business models and customer base. Collecting this data is critical, but these efforts could prove of little value if the data is not run against quality risk intelligence that is purpose-built to identify exposure to sanctions. Screening the collected data against government lists alone will not identify exposure.

70 billion

The number of digital verification checks to be conducted in 2024, an increase of 16% from the previous year.

Source: Digital Identity Verification Checks to Pass the 70 Billion Mark in 2024 (juniperresearch.com)

4   Is new technology changing the way sanctions screening works today?

Simmons

Absolutely! Newer style tech innovation is an indispensable ally for financial institutions and corporates seeking to manage sanctions risk effectively. Advanced tools assist in detecting and preventing suspicious activities. Machine learning algorithms and AI analyze vast amounts of data, flag suspicious transactions, and identify patterns of unusual behavior that may indicate potential sanctions breaches (or money laundering) in a fraction of the time that older methods require. The use of Large Language Models (LLMs) in generative AI applications helps with unstructured data and match accuracy. By harnessing these technologies, companies can proactively manage sanctions risks, improving their compliance efforts, and safeguarding their operations from the detrimental consequences of financial crimes.

Shirley

Now, more than ever, yes! Gen AI has democratized AI, speeding up software development and challenging all industries to assess how AI, both predictive and generative, can be applied to a wide array of problems. For the sanctions industry, this means the cost of detecting 100% of true positives, the regulatory obligation, and an increasing number of false positives (up to 80%) is reducing. With AI enhancements rolled out, skilled sanctions investigators have the time they need to focus on the higher impact and complex tasks.

> " Newer style tech innovation is an indispensable ally for financial institutions and corporates seeking to manage sanctions risk effectively.
>
> **– Charmian Simmons**

Princen

Yes. But we need to ensure that these new technologies are applied correctly. We believe that starting out with the application of AI alongside a rules-based engine, and then increasing the importance of the AI component over time, is the best approach. Financial institutions and especially regulators need to become confident that AI can help reduce both risk and false positives.

We have seen that our post-processing AI-based solution for sanctions screening performs very well in most scenarios but there are still cases where the machine cannot decide or when a different form of AI needs to be applied. For example, a suspicious transaction can be stopped but requires additional information that is not present. In that case, AI cannot help because it is missing vital information.

But, generative AI can help investigators in requesting that information and interpreting it when received. These are two different application areas of AI, each with their own strengths and weaknesses. Using them incorrectly can lead to compliance problems. It is important to partner up with a company that guides customers and recommends them on how AI is applied in the different phases of the alert and investigation process.

Mendelsohn

There are material efforts to address inefficiencies in sanctions screening to include addressing high false positive hit rates. Some risk management leaders are leveraging artificial intelligence, machine learning, and high-quality risk data to reduce noise. To the extent institutions are successful in reducing noise and creating efficiencies, there will be increasing bandwidth to use high-quality risk data to identify sanctions and export controls-related exposure–not only on Russia but on other high-priority national security matters that could relate to Iran, North Korea, or fentanyl and terrorist financing, among others.

> " There are material efforts to address inefficiencies in sanctions screening.
>
> **– Howard Mendelsohn**

5 **What essential advice would you offer to financial institutions and corporates on assessing technology solutions available on the market and integrating them with existing systems? What steps will ensure the process is as smooth as possible?**

Simmons

Improving the efficiency and effectiveness of sanctions and anti-money laundering (AML) compliance frameworks requires a proactive approach. First, FIs and corporates should prioritize regular and comprehensive risk assessments to identify vulnerabilities and tailor their efforts accordingly. Understanding how technology innovations such as predictive and generative AI work in one or several use cases allows for important decisions to be made in upgrading or acquiring new solutions. This includes understanding how they add business value and how they automate and streamline to address difficult and/or repetitive tasks. Ensuring strong governance and accountability is an ongoing responsibility, especially with the use of AI today, and fosters a top-down culture of compliance. Finally, maintaining adaptability and staying abreast of regulatory developments is crucial to effectively navigating the ever-evolving landscape of AML and sanctions compliance.

$85.7 billion

Expected spend on generative AI in banking by 2030, an increase of 1,430% from 2024.

Shirley

To assess and integrate technology solutions effectively, financial institutions and regulated corporates should conduct comprehensive risk assessments to identify vulnerabilities and tailor solutions accordingly. They should embrace paradigm-shifting gen AI, setting targets (e.g., 30%) for how much more operationally efficient the organization can become with its adoption.

Next, build a plan around achieving perpetual KYC, as it can enable continuous, dynamic updates of customer profiles, ensuring real-time compliance and enhancing risk management, thereby improving the efficiency of financial crime prevention. It is crucial to select technologies that integrate seamlessly with existing systems and can scale with evolving compliance demands. Prioritizing data quality and governance, ensuring accurate and up-to-date data, and establishing robust governance frameworks for AI models are essential. Starting with pilot programs to test new technologies and gather feedback for improvement, providing thorough training for staff, managing changes effectively, and staying informed on regulatory developments will ensure a smooth and effective integration of new technology solutions.

By following these steps and embracing gen AI, institutions can transform their organizations, making financial crime prevention more efficient and effective.

Princen

As mentioned before, we believe in a gradual integration of AI into an organization's screening solution. For example, our approach is to use a rules-based engine to deliver potential name hits and then use a mixture of AI and rules to determine if this is a true or false positive.

As part of a risk model, customers decide how important the AI contribution is in their decision. It can be 10% at first and move up to 90% as confidence and market readiness evolves over time. Additionally, the way AI is used must be transparent, explainable, and auditable; the model needs to be able to grow and improve. As such, model governance will become a key factor in the future.

Mendelsohn

Financial institutions and corporations should understand gaps and enhancement opportunities in control frameworks relating to sanctions, export controls, and investment restriction programs. Risk management leaders should understand the need for and role of specialized data providers to complement existing legacy providers of government lists and adverse media. As specialized providers are chosen, pilot programs should be established and appropriately resourced. Successful outcomes should be shared with senior management to educate on change management and innovation and to secure resources to scale change that will create business efficiencies, identify exposure, and materially decrease risk.

Panelist bios

Charmian Simmons
Financial Crime and Compliance Expert, SymphonyAI
www.symphonyai.com/financial-services

Charmian Simmons is a financial crime and compliance expert covering financial services at SymphonyAI. She has over 20 years of experience in the financial sector, covering risk management, financial crime, internal controls, and IT advisory. She is a technology evangelist specializing in AI innovations and transformation. Charmian is responsible for providing practitioner expertise and thought leadership and analyzing key policy, regulatory, and technology drivers that transform the compliance market. Charmian is CAMS, CDPSE, CRMA, and CISA certified.

Ben Princen
Sanctions Product Manager, SymphonyAI
www.symphonyai.com/financial-services

Ben Princen is a renowned subject matter expert in sanctions compliance. He manages the NetReveal Sanctions Screening products, steering its strategic direction and development roadmap. Ben's extensive collaboration, during his 19 years with the organization, with industry leaders has been pivotal in safeguarding them against financial crimes. His involvement in several significant and complex financial crime initiatives showcases his ability to blend technical expertise with business acumen, driving innovation and effectiveness at speed. A certified sanctions specialist (ACSS), Ben continues to shape the future of financial security with his in-depth knowledge and forward-thinking approach.

Enda Shirley
Head of Compliance, SymphonyAI
www.symphonyai.com/financial-services

Enda Shirley is head of compliance and an anti-money laundering specialist with more than 13 years of experience innovating within the financial services industry. His work at SymphonyAI includes managing the strategy and vision of its financial crime compliance products, enabling financial institutions to tackle the evolving money laundering landscape effectively and efficiently. He strives daily to solve problems by combining partner feedback and regulatory insights with bleeding-edge technology.
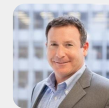
Howard Mendelsohn
Chief Operating Officer, Kharon
www.kharon.com

Howard works closely with business, compliance, and legal professionals to strengthen programs and controls for managing risks at the intersection of global security and commerce. Howard has over two decades of experience in combating illicit financial activity in both the government and the private sector. Howard served at the US Treasury Department from 2001 to 2011, including as deputy assistant secretary and assistant secretary (acting) for the Treasury Department's Office of Intelligence and Analysis. Howard led the Treasury Department's intelligence functions, including oversight of analytical production, risk assessment, security, and strategic planning. Following his service at the Treasury Department, Howard held leadership positions in enterprise compliance at PNC Financial Services Group. He is a recognized thought leader on global security and risk matters and speaks regularly at conferences.

About Kharon

Kharon helps leading organizations identify a range of sanctions and compliance risks, critical to managing financial crimes, supply chain exposure, export controls, investment risk, and more. In May, it was announced that the US Department of the Treasury and Kharon had signed a contract giving officials within the Treasury Department access to Kharon's global risk analytics platform.

Learn more at www.kharon.com

About SymphonyAI

SymphonyAI, 2024 Microsoft Partner of the Year for Business Transformation – AI Innovation, is building the leading enterprise AI SaaS company for digital transformation across the most critical and resilient growth verticals, including retail, consumer packaged goods, finance, manufacturing, media, and IT/enterprise service management. SymphonyAI verticals have many leading enterprises as clients. Since its founding in 2017, SymphonyAI has grown rapidly to 3,000 talented leaders, data scientists, and other professionals. SymphonyAI is an SAIGroup company, backed by a $1 billion commitment from Dr. Romesh Wadhwani, a successful entrepreneur and philanthropist.

SymphonyAI provides AI-focused SaaS solutions developed from the ground up for fighting financial crime. An end-to-end offering compiled from more than 25 years of knowledge in tackling money laundering and fraud, our award-winning product ecosystem comprises an innovative and modern approach to financial crime investigation using world-leading predictive and gen AI. From KYC/CDD and transaction monitoring to payments fraud, entity resolution, sanctions, PEP, and adverse media screening, SymphonyAI is a trusted name in finance technology, with more than a third of the world's top 100 banks enjoying the power, efficiency, effectiveness and productivity that our solutions provide.

Learn more at www.symphonyai.com.