# Keeping pace with geopolitics and sanctions

fintrail.com

lynxtech.com

White Paper

Lynx

FINTRAIL

# Keeping pace with geopolitics and sanctions

Sanctions have increasingly become strategic weapons to tackle global threats and political shifts head-on. The UK government has called sanctions a "critical instrument of the UK's foreign, national and security policy" in a "more dangerous and uncertain world".[1] The EU has described its use of sanctions as a "preventive and non-punitive instrument that allows the EU to respond swiftly to political challenges and developments".[2]

While geopolitical developments and sanctions go hand-in-hand, it is the private sector - and in particular financial institutions - that are tasked with implementing them. Financial institutions must be ready to respond and implement at a moment's notice when new sanctions designations are announced - from screening their customer base against new designations to ensuring that they have controls in place to detect and disrupt sanctions evasion.

With often leaner compliance teams and more innovative financial products, emerging financial service firms have in particular felt the sanctions compliance pressure in recent years. For many Fintechs, sanctions have gone from being a simple screening check done at onboarding to the

1 UK Government

2 The Diplomatic Service of the European Union

need for ongoing due diligence, screening and monitoring to detect sanctions evasion attempts and stay on top of regulatory developments. Being able to maintain efficient sanctions screening controls - no matter the number of designations - is key for enabling Fintechs to scale and instill confidence with banking partners who Fintechs often rely on to service their customers.

Regulators increasingly expect firms to adapt their screening systems to the sanctions risks they face and the geopolitical environment they operate within. In their 2023 sanctions systems and controls thematic review of firms, the FCA noted that many firms have "poorly calibrated or tailored screening tools" that were not calibrated to the risks faced by a firm.[3] OFAC, in its 'Framework for OFAC Compliance Commitments', similarly noted that firms should implement controls that are calibrated to the firm's risk profile[4], while the European Banking Authority as recently as November 2024, called on firms to adapt screening systems to the size, nature and complexity of a firm and its sanctions risk exposure.[5]

This paper examines the delicate relationship between geopolitics and the sanctions screening controls deployed by financial institutions and identifies strategies Fintechs can use to stay ahead of sanctions and adapt their screening systems to screen more efficiently in response to the geopolitical crises of tomorrow and in line with sanctions risks.

> "Being able to maintain efficient sanctions screening controls - no matter the number of designations - is key for enabling Fintechs to scale and instill confidence with banking partners who Fintechs often rely on to service their customers."

## An ever-changing sanctions landscape

Sanctions screening has historically been treated as a largely reactive and simple exercise: when new persons or entities are added to a sanctions list, the updated lists are screened against a firm's customer base and potential matches are flagged. This approach, however, does not account for the individual sanctions risks faced by a firm. It may result in a high number of false positive alerts or the risk that sanctioned persons will simply evade sanctions through third parties or falsified information, and leaves firms unprepared for the complexities of managing their sanctions exposure.

3 FCA - Financial Conduct Authority

4 OFAC - Office of Foreign Assets Control

5 EBA – European Banking Authority

## Sanctions horizon scanning

Staying abreast of sanctions developments can help firms stay one step ahead and tailor their screening controls to the specific sanctions risks they face.

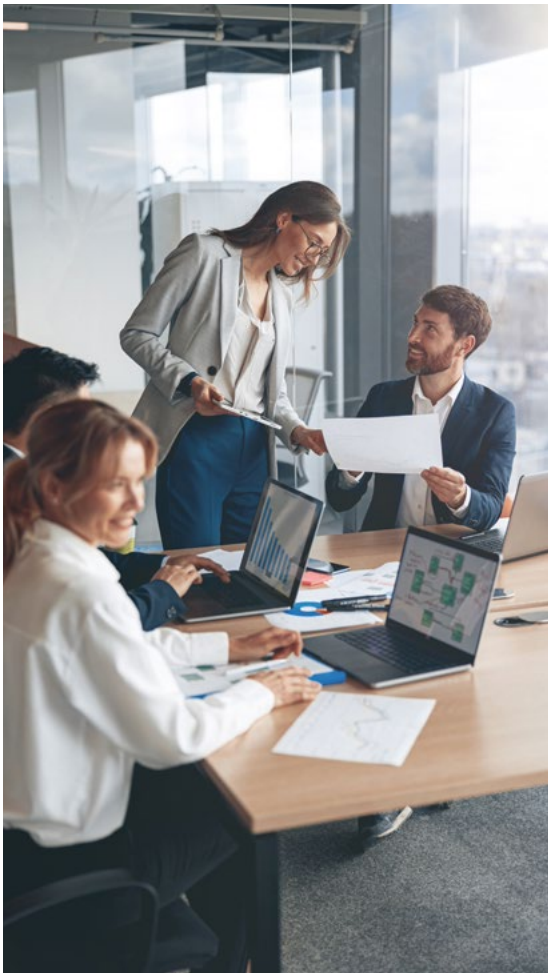
For example, in October 2022 the European Union made the decision to prohibit the provision of all crypto-asset services to Russia, necessitating a full withdrawal from Russia by EU-based crypto firms.[6] The EU's crypto measures of October 2022 were, however, preceded by an initial ban on high-value crypto-asset services in April 2022 and by numerous news stories that Russia could be using cryptocurrency to evade sanctions.[7]

Firms who saw the writing on the wall and understood their exposure to Russian crypto markets were better prepared to implement resultant sanctions measures. Understanding - and predicting - how your firm is exposed to changing sanctions events is therefore key.

The Financial Conduct Authority in 2023 noted that UK firms that had "conducted risk exposure assessments and scenario planning in advance of the Russian invasion of Ukraine" were "better placed to manage the resulting demands".[8]

Sanctions horizon scanning involves considering geopolitical developments - what countries are likely to become sanctions hotspots, what sanction evasion typologies are likely targets of new sanctions - and how these overlap with your firm's customers (for example, payments to countries neighbouring heavily sanctioned jurisdictions) or products (for example embedded banking where nested relationships may be higher risk for sanctions evasion schemes).

In addition to geopolitical analysis, sanctions horizon scanning involves an understanding of evolving regulatory frameworks and tracking enforcement actions. New sanctions restrictions may target specific sectors of the economy or activities, and enforcement actions will provide insight into what controls regulators expect firms to have in place. For example, a recent trend in OFAC enforcement actions has been on screening IP addresses. OFAC's 2022 fine against Kraken, focused on the fact that Kraken screened IP addresses at onboarding, but did not for subsequent transactions carried out by the customer, emphasised the need for financial institutions to consider all available data points in screening to detect sanctioned activities and jurisdictions in addition to sanctioned persons.



6 European Commission

7 The Guardian

8 FCA - Financial Conduct Authority

# Case example:

## Unpicking the complexities of sanctions and geopolitics

One clear example of the dynamic between geopolitics and sanctions is US sanctions against Venezuela. While sanctions against Venezuela date back some 20 years, in recent years the interplay between political developments on the ground and US sanctions is starker than ever: In October 2023 a process began whereby the US provided sanctions relief in return of the promise by President Maduro to introduce free and fair elections in Venezuela, and a cat and mouse game of political developments and sanctions actions began.

| | Development | Action |
|---|---|---|
| 2023 | **October 2023:** President Maduro and the opposition signed the Barbados Agreement for a roadmap for free and fair elections in Venezuela. | The US issues licenses authorizing transactions with Venezuela's gold and oil & gas industry for an initial 6 months (April 18, 2024). |
| | **December 2023:** The Maduro government agrees to allow opposition candidate Maria Machado to appeal her previous disqualification from the election.<br>Venezuela releases 20 Venezuelan and 6 US political prisoners. | |

| | Development | Sanctions Action |
|---|---|---|
| 2024 | **January 2024:** Supreme Court upholds ban on the candidacy of Maria Machado. | The US revokes license on Venezuelan gold. |
| | **April 2024:** Maduro's government continues to violate the Barbados Agreement, including the arrest of civil society, journalists and opposition figures. | The US announced it will not renew oil & gas licenses due to Maduro's failure to meet the agreed terms of the Agreement. |
| | **July 2024:** Venezuela holds elections, which are widely disputed. Maduro is sworn into office in January 2025. | Throughout 2025, the US, UK, EU and Canada issue coordinated sanctions, including the president of Venezuela's state-owned oil company and high-level government and police officials, citing Maduro's "*continued violent repression in an attempt to maintain power*". |

For the private sector, changing political priorities impacts screening efforts. Effective screening requires accurate and up-to-date screening lists, and screening configuration that is tailored to the risks. This includes:

## List updates

In response to ever-changing designations - where persons and entities may be added and removed from lists, or ownership and control changes - financial institutions should be confident that they are always screening against the latest version of the sanctions list. While screening providers may provide the list, firms should be able to verify that the provider's list is updated and - crucially - screened against the firm's customer database.

## Naming conventions and fuzzy matching

The ability to detect variations in names is crucial for effective screening and ensuring these are tailored to the naming conventions or scripts of targeted countries or countries where the firm's customer base is located. Venezuelan names follow a Spanish naming convention where a person's given name is followed by both a paternal and maternal family name.

## Ownership structure

Screening the names on a sanctions list is only one half of the puzzle. The ability to detect entities that are owned or controlled by sanctioned entities in Venezuela's oil and gas sector, or part of specific sectors of the economy benefiting from Venezuela's government requires both good customer data obtained through customer due diligence that maps ownership and control, and good screening solutions that can screen against these.

## Detecting sanctions evasion


Firms must be alert to changing sanctions evasion tactics deployed by sanctioned targets to develop screening and transaction monitoring systems able to identify activity indicative of sanctions evasion, for example by routing payments related to Venezuela's prohibited sectors through third countries or using non-fiat transfer methods.

## Combining name screening with additional data points

Including IP addresses, physical addresses, website domains, phone numbers, email addresses and keyword screening to detect exposure to Venezuela's oil and gas or gold sectors.

# Calibrating screening systems to sanctions risks

Firms are increasingly expected to calibrate their screening systems to the specific sanctions risks that they face, and not simply rely on out-of-the-box tooling with little ownership and oversight of the tool.

## More than just sanctioned names

As sanctions ramped up against Russia in 2022, many Fintechs made adjustments to their sanctions screening systems in response to the increased sanctions risk from Russia. This included enhancing client due diligence to understand complex ownership structures of corporate clients to detect direct or indirect links to Russia, and upgrading screening systems in response to Russia-related risks.[9] In addition, many Fintechs made the decision to make Russia a prohibited country, which necessitated an expansion of screening system capabilities beyond simply complying with sanctions restrictions to being able to detect any Russian nexus on customers or payments, not just sanctioned exposure.

When thinking about the customisations available to firms in screening systems, this may include:

### List selection and list management

The lists that firms wish to screen against should be tailored to where firms are regulated, where their customers are based, their products as well as risk appetite. Choosing what lists to screen against is not a one-off exercise, but is instead an ongoing process to ensure firms stay compliant and manage their sanctions risks. Fintechs should keep in mind that the more lists screened, the more potential false positive alerts can be generated. Firms should carefully consider what lists the firm must comply with due to its regulatory obligations, and what lists the firm *wants* to comply with due to its risk appetite. In addition, firms should consider what lists are likely to produce true matches that are significant to the firm.

For example, a US-based Fintech specialising in cross-border payments to France may choose to screen against a wider selection of lists, to address the additional sanctions exposure that comes from sending and receiving cross-border payments, versus a Fintech offering only domestic payments to US-based customers.

[9] Insights gathered from FINTRAIL clients, see 10 Principles for Sanctions Preparedness

As of February 2025, OFAC's SDN list included names of over 11,000 individuals and 13,000 entities and remains by far the most comprehensive sanctions list in terms of number of designations and geographic reach. Other lists, however, may be just as useful for firms with exposure to certain countries - such as France's autonomous asset freeze list which includes names of persons involved in terrorist activity in France.

## Matching algorithms

How customer names are matched against the sanctions list matters and most firms will want to be able to detect small variations in spelling that may be introduced through customer due diligence processes, local naming conventions or obfuscation by sanctioned parties.

Firms should be aware that fuzzy matching algorithms will differ from each screening system, but is often a combination of the number of changes required to make one word into another, the number of matching characters between two words and words that sound similar but are spelled differently. This is combined to a composite matching score between two names, often represented as a percentage. The names Vladimir Putin and Volodimir Putin have a 96% OFAC match score and are deemed similar due to their phonetic matching and alternative spelling of the same name, whereas Waldemar Putin is a 59% match suggesting the names are less similar.

Firms are responsible for determining what level of fuzzy matching they wish to apply to their screening, and again this should be directly informed by the sanctions risks they face. Where sanctions risk is higher, firms will want to pick up more potential matches and therefore decrease the fuzziness level.

Firms must also ensure that their matching algorithms are sufficient for the markets they operate in, or the products they provide. For example, operating in countries with non-latin scripts will require the screening software to pick up non-latin characters and transliterate these correctly into their latin form.

A Chinese surname can be spelled differently depending on the specific characters used, or due to different dialects - for example the character for "Zhang" can also be romanized as "Chang" or as "Cheung" in Cantonese. Moreover, Chinese names are often listed as a surname first, followed by a given name. For Russian names, screening systems should adequately account for patronymics - the middle name indicating whether a person is a son or a daughter, whereas Spanish names use both a paternal and maternal surname that should be considered. Therefore, traditional matching algorithms focusing solely on the similarity between two name strings may not be sufficient for every naming convention.

## Risk-based approach to screening

The calibration of screening systems is often done firm-wide, but as firms mature they may adopt a more granular approach that segments screening based on customer demographics, product types and geographical exposure to allow for a more targeted and customised screening approach. Customers and payments with links to high-risk jurisdictions or industries may have stricter screening and filters, whereby closed-loop products (where the payments relating to the product will only involve the firm's own customer) may present a lower sanctions risk.

While many firms make use of a risk-based approach to screening, and this being increasingly expected by regulators,firms should note that they may still be penalised for sanctions breaches resulting from implementing a risk-based approach.

In addition, firms should be aware that the more customisations they introduce, the more opportunity for errors. Firms should keep an audit trail of any customisations made to the firm's screening configuration in order to be able to explain the reasoning for these decisions to the regulator. It is important that firms have carefully considered sanctions risk exposure and are able to explain why screening configurations applied either firm-wide or to specific products and use cases are linked to sanctions risk. Crucially, while a risk-based approach may result in fewer false positive alerts being generated, this should not be the reason for introducing a risk-based approach to screening.

### **Case study:** Starling Bank[10]

In November 2024, the Financial Conduct Authority fined Starling Bank for various financial crime failings, including significant gaps in its screening controls. This included only screening its customers against a subset of the UK sanctions list, and only screening customers every 14 days. The FCA deemed this was not keeping up with "current industry standards". Crucially, the FCA noted that the firm had failed to take into account its financial sanctions risks in making these decisions, and that the firm did not adequately consider areas of higher risk exposure such as payments from crypto exchanges or multi-currency accounts.

[10] FCA - Financial Conduct Authority

# Technology can help scale screening

Resourcing is key for effective sanctions screening. The FCA highlighted that "sanctions teams need to be properly resourced to avoid backlogs ... and enable a quick reaction to sanctions risks" and noted that a lack of resources in operational teams had resulted in "a lack of clarity on prioritisation of alerts" and prevented firms from "taking appropriate and timely action". Amidst a changing geopolitical landscape, firms must be ready to respond to upticks in sanctions alerts and direct resources to where the risk is highest.

Resourcing includes both human resources and technology, and the latter category is particularly important for Fintechs who operate with leaner teams and pressure to scale efficiently - while staying compliant. Technologies such as artificial intelligence (AI) and machine learning tools can be deployed to screen smarter.

At the alert generation stage, technology, such as advanced natural language processing (NLP), could be used to enrich watchlist databases with more name variations to ensure comprehensiveness. Advanced NLP and AI models can also collaborate to enhance name scoring by intelligently selecting and applying the most effective NLP algorithms for each name comparison. Last but not least, highly configurable solutions can also combine the potential name match with other customer attributes - such as citizenship, date of birth or IP address - to validate the likelihood of a true match and use this to prioritise alerts for review, helping compliance teams focus finite resources where the risks are higher.

If a Fintech is able to demonstrate to banking partners that a sanctions screening system is tuned to the firm's sanctions risks, this can instill the confidence with the banking partner necessary to scale and build new products.

The possibilities of technology should however always be balanced with the high regulatory enforcement risk that comes with sanctions. While some firms may explore possibilities of models making decisions on alerts, it is important that such decisions are explainable to the regulator. Should a breach occur as a result of an artificial intelligence decision, regulatory scrutiny may be higher.

# Key actions for Fintechs

Compared with larger financial institutions, Fintechs often operate with leaner compliance functions and some Fintechs may not have a standalone sanctions compliance function. However, even with limited resources and time available, sanctions horizon scanning and tailored screening controls does not have to be a daunting task. Below are three key steps for Fintechs to consider when it comes to adopting a more proactive approach to screening stays ahead of geopolitical developments.

## 01 Designate a person responsible for sanctions horizon scanning.

One member of the team should have the responsibility for staying abreast of new sanctions regulatory developments that may impact the firm's customers or products. This can include signing up to sanctions-related news services[11], staying up to date with guidance and enforcement notices released by sanctions agencies in the UK, US and EU member states, or taking part in industry forums such as the Fintech Fincrime Exchange or the FINTRAIL Sanctions Club[12] to stay informed of key sanctions designations and emerging sanctions trends.

[11] For example GlobalSanctions.com which provides a daily roundup of sanctions developments.

[12] FINTRAIL Sanctions Club & FINTRAIL - FFE

# 02 Ensure emerging sanctions risks are considered in the firm's financial crime risk assessment.

A risk assessment should consider both current risks, as well as risks that have the potential to materialise in the near future. The firm's risk assessment should consider emerging sanctions evasion typologies (for example sanctions evasion through third countries) or scenarios (the risk that sanctions are ramped up in a country the firm has significant exposure to). Firms should think about how their products and customers overlap with what is known about these emerging sanctions risks to determine the firm's inherent risk exposure, and any relevant controls already in place that mitigates this risk.

# 03 Take it one step at a time.

If firms identify an area of high sanctions risk exposure, firms should carefully consider how screening controls already in place can be enhanced or configured to mitigate the risk. By carefully testing the impact of any screening enhancements before they go live, firms can avoid generating too many false positive reviews and instead have a more targeted approach to screening additional filters. Conversely, if firms identify areas where the sanctions risk is lower, the knee jerk reaction may be to immediately turn off screening controls. However, firms should remember that screening controls should be viewed as dials that can be dialled up or down in line with risk, rather than turned on or off completely. This will allow firms to gradually reduce screening controls (higher fuzzy matching thresholds, additional whitelisting and suppression, fewer lists) rather than turning off screening controls completely. Gradually dialling screening controls up or down in line with sanctions risks will allow firms to ensure true matches are still detected.

To navigate the ever-shifting sanctions landscape, financial institutions, and particularly Fintechs, must move beyond reactive screening processes. By embracing a proactive sanctions approach which includes horizon scanning, understanding the interplay between geopolitics and sanctions, tailoring screening systems to emerging sanctions risks, and utilizing a proportionate risk-based approach, firms can significantly enhance their sanctions compliance efforts.

## About FINTRAIL

FINTRAIL's experts have extensive knowledge of sanctions regulatory requirements and their application in practice. We can assist clients of all sizes build and maintain a sanctions compliance programme. This includes:

- Bespoke advice on sanctions compliance issues, as well as regulatory mapping and horizon scanning.
- Development or enhancement of sanctions policies and procedures
- Model validation, testing and assurance of screening tools, and provide advice on how to optimise sanctions screening.

To find out more, visit
**www.fintrail.com/sanctions-services**

## About Lynx

Lynx is an AI-driven software company designed to solve clients' most significant challenges in fraud and financial crime. Our AML screening platform combines instant payment and customer screening, advanced AI-driven risk detection, and seamless API integration to streamline compliance while minimizing friction for legitimate transactions. With configurable workflows, intelligent automation, and millisecond response times, Lynx empowers organizations to stay ahead of evolving regulations and strengthen their financial crime controls.

Learn more at
www.**lynx**tech.com.

Lynx

## Contact Us

**Get in touch with us:**

**Website:** **lynx**tech.com

**Email:** info@lynxtech.com

## Recognitions

Recognised as a Representative Vendor in **Gartner® Market Guide for Fraud Detection in Banking Payments: 2024**

Named as a Sample Vendor in **Gartner® Emerging Tech Impact Radar: 2025**

Anti-Fraud Solution of the Year at the **FStech Awards**

Chartis Financial Crime and Compliance50 2024

Chartis RiskTech Quadrant® Category Leader Enterprise Fraud Solutions, 2024

Chartis RiskTech Quadrant® Category Leader Payment Fraud Solutions, 2024

Chartis RiskTech Quadrant® Best of Breed Name and Transaction Screening Solution, 2024

datos INSIGHTS

CBINSIGHTS Fintech 100 2024