

Insights

NEW OFSI DECISION GIVES BEST GUIDANCE YET ON SANCTIONS DUE DILIGENCE

Feb 04, 2026

SUMMARY

On 26 January 2026, the Office of Financial Sanctions Implementation (“**OFSI**”) provided its clearest guidance yet on the baseline level of due diligence it expects businesses to undertake when assessing sanctions risks.

Below we draw out the key compliance and due diligence considerations for businesses in light of OFSI’s [penalty notice](#) (the “**Notice**”) following the imposition of a £160,000 fine on a UK-registered bank (the “**Bank**”) for breaching the Russia (Sanctions) (EU Exit) Regulations 2019 (*SI 2019/855*) (the “**Regulations**”).

BACKGROUND

Between 8 and 24 February 2023, the Bank processed 24 payments totalling £77,383.39 to or from a personal current account held by an individual customer designated under the Regulations (the “**DP**”). The breaches occurred because the DP opened the account using a UK passport containing a common transliteration-based spelling variation of their name, and the Bank’s sanctions screening system lacked sufficient enhancements to identify and reconcile that variation.

The breaches were discovered when a Politically Exposed Persons (“**PEP**”) alert was triggered after the name variation matched an entry on the Bank’s parent company’s commercial PEP list. A manual adverse-media review then identified the DP. The absence of clear escalation procedures for potential sanctions matches further aggravated the position - an issue OFSI highlighted as particularly significant given the overlap between DPs and PEPs.

On 16 March 2023, the Bank’s parent company notified OFSI of the breaches on the subsidiary’s behalf. As a result, OFSI granted the maximum 50% voluntary disclosure discount permitted under its Enforcement Guidance.

KEY COMPLIANCE AND DUE DILIGENCE TAKEAWAYS

Enhanced Screening for High-Risk Firms

The Notice clarifies OFSI's expected level of compliance; firms with heightened exposure to sanctions risks should implement proportionately enhanced screening measures. Although OFSI does not require firms to procure commercial sanctions lists, entities operating in higher-risk environments are expected to strengthen their sanctions lists, whether by adopting commercial solutions or implementing robust in-house enhancements. As per the Notice, ultimate responsibility for sanctions compliance rests with the entity committing the breach. While compliance activities might be delegated to group functions or external providers, that does not transfer legal responsibility. In effect, therefore, outsourcing compliance processes does not equate to outsourcing accountability.

In this case, OFSI observed that the Bank did not identify the spelling variation of the DP's name, despite holding this information through its PEP screening processes. The absence of a commercial sanctions list at the time of the breach, combined with the Bank's failure to enhance its sanctions screening using information already available to it, was treated as an aggravating factor. This highlights the importance of regularly reviewing and updating sanctions lists using multiple reliable sources, particularly where translation issues may arise. OFSI also emphasises the *"inherent risks associated with automated sanctions screening"* making it essential for firms to maintain robust and clearly defined contingency procedures.

- **Assess whether your sanctions risk profile (geographic exposure, customer base, transaction types) requires commercial list enhancement.**
- **Test screening systems for transliteration and character-set variants, particularly in relation to higher-risk jurisdictions (e.g., Russia, China, and Arabic-speaking countries).**
- **Ensure screening tools can reconcile common character equivalents and spelling variations resulting from translation.**
- **Review whether information captured in one compliance system (PEP, AML, KYC) could enhance sanctions screening, noting OFSI's expectation that firms use *"all relevant and available information"* within their possession.**

Escalation Procedures

The Notice also identified the absence of clear procedural guidance requiring staff to escalate potential sanctions connections identified during PEP checks as an aggravating factor. OFSI emphasised that *"internal policies should provide robust and explicit guidance to staff regarding the escalation of potential sanctions concerns,"* particularly in higher-risk areas of the business, such as those involving PEPs. Firms should ensure that escalation pathways are clearly defined so that any potential sanctions issues - especially those relating to potential DPs - are promptly referred to the appropriate team.

- **Update PEP, AML, and KYC procedures to include mandatory escalation protocols to your sanctions team for any potential sanctions connections. Consider making this explicit in written procedures and training.**
- **Ensure clear internal procedures are in place for identifying, investigating, and promptly disclosing potential sanctions breaches to OFSI.**

Training

Finally, the Notice highlights the importance of regularly reviewing and updating training materials to ensure they reflect current regulatory and geopolitical developments. In this case, the Bank's mandatory and advanced training modules were outdated, which OFSI treated as an aggravating factor. By contrast, maintaining up-to-date training is a straightforward compliance measure and may be recognised as a mitigating factor in any future enforcement action.

- **Undertake a review of sanctions training materials to ensure they are up to date and reflect current regulatory and geopolitical developments.**

DILIGENCE GUIDANCE FROM ACROSS THE POND

When it comes to ensuring compliance with U.S. sanctions regulations, the U.S. Office of Foreign Assets Control ("**OFAC**") has provided official [guidance](#) for U.S. firms regarding sanctions screening tools. The guidance specifically discusses the use of "false hit lists," which automatically suppress screening alerts triggered by individuals and entities who are not actually subject to sanctions but have similar names as sanctioned persons. The guidance came after an OFAC enforcement action against a U.S. financial institution that placed a customer for which an OFAC general licence authorized transactions on a "false hit list." However, the general licence expired, but the financial institution did not remove the customer from the "false hit list," resulting in continued engagement with the sanctioned customer without any type of OFAC authorization. While OFAC recognizes that developing a "false hit list" can be an efficient and legitimate screening strategy, OFAC's guidance cautions that these tools may be unreliable if not regularly reviewed and updated. Like the OFSI Notice, OFAC recommends companies and financial institutions implement specific measures to keep their screening programs accurate and thus avoid potential violations or enforcement actions.

- **Conduct periodic reviews of false hits lists.**
- **Ensure screening alerts generated in connection with additions/changes to OFAC's sanctions lists (e.g., Specially Designated Nationals and Blocked Persons List) are not automatically suppressed by an existing, similar false hit list entry.**
- **Amend false hit lists as needed in response to updates to OFAC sanctions programs.**

- For direct customers with a false hit list entry, ensure any meaningful changes to the customer's information (e.g., address, ownership status, business activity) trigger review of the entry.

CONCLUSION

This guidance from OFSI on its minimum due diligence expectations (which is likely to be of a higher standard than many businesses will have anticipated) is a welcome addition to the sanctions compliance toolkit. Companies may wish to use the Notice (and related OFAC guidance) as an opportunity to review and refresh their screening and due diligence processes. Both frameworks demonstrate the importance of implementing supplemental screening processes, especially for firms engaging across multiple languages or translations. Failure to have accurate screening and due diligence processes in order can cause downstream disruption, as mistaken approvals or unresolved alerts may be identified later by other parties in the transaction chain, leading to unnecessary delays, in particular where banks' mandatory reporting obligations are triggered where a potential sanctions breach is detected.

If you have any queries or would like to discuss these developments further, please contact your usual contact or any member of the team: [Chirs Bryant](#), [Alexis Early](#), [Sonja Hainsworth](#), [Adam Harper](#), or [Grace Driskell](#).

The authors would like to thank Trainee Solicitor Ella Hume for her contribution to this article.

RELATED CAPABILITIES

- Antitrust & Competition

MEET THE TEAM



Chris Bryant

Partner, London / Brussels

chris.bryant@bclplaw.com

[+44 \(0\) 20 3400 2423](tel:+442034002423)



Alexis Early

Partner, Washington

alexis.early@bclplaw.com

[+1 202 508 6089](tel:+12025086089)



Sonja Hainsworth

Counsel, London

sonja.hainsworth@bclplaw.com

[+44 \(0\) 20 3400 3713](tel:+442034003713)



Adam Harper

Counsel, Washington

adam.harper@bclplaw.com

+1 202 508 6090

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.