Office of Financial
Sanctions Implementation
HM Treasury

Report Concerning Breach of Financial Sanctions
Regulations (section 149(3) PACA 2017 report)

Publication of a Report – Wise Payments Limited

Summary

1. On 31 August 2023 the Office of Financial Sanctions Implementation (OFSI), part of HM Treasury, issued this report in accordance with s149(3) of the Policing and Crime Act 2017 ("PACA") against Wise Payments Limited ("Wise") for breaching regulation 12 of The Russia (Sanctions) EU Exit Regulations 2019 ("the Russia Regulations"). OFSI refers to the use of this power as a Disclosure.

2. Wise is a UK registered company, regulated by the Financial Conduct Authority (FCA), providing financial services to consumers and businesses.

3. This Disclosure relates to a cash withdrawal of £250 made from a business account with Wise held by a company owned or controlled by a person designated under the Russia Regulations ("the Designated Person"). In permitting the withdrawal, Wise made funds available to a company owned or controlled by a designated person.

4. OFSI categorises breach cases as being of lesser severity, moderate severity or serious enough to justify a civil monetary penalty. On the facts as known, OFSI does not assess the breach as sufficiently serious to impose a monetary penalty on Wise. However, the nature and circumstances of this breach were assessed as moderately severe and in OFSI's judgement a Disclosure is the appropriate and proportionate enforcement response.

5. We consider that this breach satisfies the test at section 149(3) of PACA 2017 which states:

> *"The Treasury may also publish reports at such intervals as it considers appropriate in cases where—*
>
> *(a) a monetary penalty has not been imposed under section 146 or 148, but*
>
> *(b) the Treasury is satisfied, on the balance of probabilities, that a person has breached a prohibition, or failed to comply with an obligation, that is imposed by or under financial sanctions legislation".*

6. OFSI notes that Wise self-reported the breach to which this Disclosure relates, and since reporting the breach, Wise has taken steps to improve the aspects of its sanctions compliance process which led to the breach occurring. These are mitigating factors for Wise.

Detail

7. On 31 December 2020, the UK financial sanctions regime in relation to the Russian Federation came fully into force, to ensure that certain sanctions relating to Russia continued to operate effectively following the UK's exit from the European Union. The UK also imposed new measures and designations in response to Russia's invasion of Ukraine in February 2022.

8. The sanctions regime is aimed at encouraging Russia to cease actions destabilising Ukraine or undermining or threatening the territorial integrity, sovereignty or independence of Ukraine. The restrictive measures set out in the Russia Regulations are intended to prevent certain Russian individuals, entities, companies, and their subsidiaries from accessing and using their assets.

9. On 20 July 2022 Wise reported a suspected breach to OFSI: on 30 June 2022, a £250 cash withdrawal was made from a Wise business account held by a company owned or controlled by the Designated Person, using a debit card held in the Designated Person's name. At that time, the company was a customer of Wise. The Designated Person was designated on 29 June 2022.

10. Wise made complete disclosures and fully cooperated with OFSI throughout its investigation.

11. The information reported and otherwise obtained from Wise indicated that at the time of the cash withdrawal, Wise's policy mandated that all customer details (including ultimate beneficial ownership/directorship of a business account) were screened against OFSI's consolidated list of sanctioned persons and entities (using a third-party sanctions data provider and Wise's in-house screening software). In the event that the screening system detected a potential sanctions match, an alert was created and the customer's profile suspended (preventing the customer from sending or receiving any funds from or to the account). If a customer had a debit card, Wise's policy at the time however was not to suspend the use of the debit card as part of the initial profile suspension process. Instead, customers would retain access to their debit cards until sanctions profile matches were resolved.

12. Wise explained to OFSI that this policy was in place because of a high false positive rate for sanctions alerts and was therefore intended to take into consideration both its regulatory requirement to pay due regard to the interests of its customers and treat them fairly, and its legal obligations to comply with financial sanctions.

13. The Designated Person was added to OFSI's consolidated list at 11:05 AM on 29 June 2022.

14. At 00:59 AM on 30 June 2022, Wise's third-party sanctions data provider added the Designated Person to its sanctions list in response to OFSI updating the consolidated list.

15. At 04:20 AM that same day, when Wise's customer base was screened following the update, Wise's systems raised an alert due to a possible name match with the Designated Person. Wise followed its policy in place at the time, so the account associated with the Designated Person was suspended following a name match alert. This prevented transfers into and out of the account but did not restrict activity on the debit card associated with the account while the potential match was being investigated.

16. At 07:25 AM on 30 June 2022, an employee of the Designated Person's company successfully withdrew £250 in cash using the debit card. By permitting the withdrawal, Wise made funds available to an entity owned or controlled by a designated person and subject to an asset freeze in breach of regulation 12 of the Russia Regulations.

17. On Friday 01 July 2022 at 05:24 AM a Wise agent reviewed the previously generated alert and determined that it was a likely true name match and, in accordance with Wise's escalation policy, further escalated this matter to Wise's sanctions specialist team. However, the escalation was not reviewed that day and at the time of the breach the sanctions specialist team did not operate weekend working.

18. As a result, it was not until 11:02 AM on Monday 04 July 2022 that a Wise agent further reviewed this transaction and then blocked the Wise-issued debit card (preventing it being used to purchase items or withdraw funds).

19. Following full suspension of the account and debit card associated with the Designated Person Wise exited the customer on 04 July 2022.

20. OFSI gave Wise notice of its intention to publish a Disclosure in relation to its breach of financial sanctions and offered Wise the opportunity to make representations. OFSI

reviewed these representations and determined that they did not alter its assessment of the breach or the nature of the appropriate enforcement action.

21. Despite the low breach value, OFSI considered that Wise's systems and controls, specifically its policy surrounding debit card payments, were inappropriate. This factor made the case moderately severe overall and enabled funds to be made available to a company owned or controlled by the Designated Person.

22. In determining this, OFSI recognised the mitigating factors in favour of Wise in this case, including the low value of the breach, the presence of voluntary disclosure, complete disclosures made to OFSI by Wise in response to requests for information, a lack of evidence of deliberate sanctions evasion and the remedial actions taken by Wise following the breach which included exiting the Designated Person as a customer, recruiting additional staff and introducing weekend working for the specialist sanctions team. Wise also changed its policy with respect to debit cards, such that both a customer's account and any associated cards are immediately blocked pending review by the specialist sanctions team where there is a possible name match with a designated person.

Notes on compliance

23. Companies and individuals must ensure they do not make funds available to designated persons or entities owned or controlled by designated persons. Wise's policy at the time of the breach (of not restricting debit cards where a possible name match to a designated person was identified) was inappropriate in managing sanctions risks. A lack of staff availability to review sanctions alerts at weekends also led to a material delay in the proper restrictions being placed on the Designated Person's account and debit card.

24. This case demonstrates that firms should carefully consider what steps are appropriate to manage their sanctions risk exposure. When a firm identifies a sanctions risk, it should take steps to fully address that risk by promptly restricting all forms of access to funds or economic resources. Firms should also maintain proportionate sanctions screening and alert review functions including, for example, at weekends where they conduct business at such times.

25. If you know or believe you have committed a breach of financial sanctions, you should inform OFSI as soon as practicable. OFSI values voluntary disclosure and if done by the

person who has committed a breach this may be considered a mitigating factor when OFSI assess the case.

26. If you are in possession or control of, or are otherwise dealing with, the funds or economic resources of a designated person you must:
    - freeze them
    - not deal with them or make them available to, or for the benefit of, the designated person, unless:
        i. there is an exception in the legislation that you can rely on; or
        ii. you have a licence from OFSI
    - report them to OFSI

27. Further information and guidance on UK financial sanctions can be found on OFSI's website: https://www.gov.uk/government/organisations/office-of-financial-sanctionsimplementation.