Imposition of Monetary Penalty – Citibank, N.A., London Branch ("CBNA London")

SUMMARY

1. On 11 August 2026, the Office of Financial Sanctions Implementation ("OFSI"), part of HM Treasury, imposed a penalty of £4,732,830.58 on CBNA London, in accordance with section 146 of the Policing and Crime Act 2017 ("PACA").

2. The penalty was imposed for breaches of the Russia (Sanctions) (EU Exit) Regulations 2019 ("the Russia Regulations") and the Global Anti-Corruption Sanctions Regulations 2021 ("the GAC Regulations").

3. OFSI assessed all breaches referred to in this notice together and made a decision on their overall seriousness. OFSI imposed a monetary penalty on CBNA London because it was satisfied, on the balance of probabilities, that CBNA London had breached prohibitions imposed by financial sanctions legislation.

4. The majority of the breaches in this case occurred between February and November 2022, following Russia's illegal invasion of Ukraine on 24 February 2022. CBNA London had particularly high exposure to future Russia sanctions risks in February 2022 due to its Russian client base, correspondent banking operations involving Russian financial institutions and payments relating to its Russian affiliate, AO Citibank (which has since been sold by Citi).

5. OFSI recognises that the significant and impactful packages of sanctions introduced by the UK and its allies in 2022 in response to the invasion presented significant operational challenges for firms with exposure to Russia. OFSI took this context into account when assessing the breaches in this case and, for the reasons set out in full in this notice, considers that these breaches nonetheless warranted the imposition of a monetary penalty.

6. The case relates to multiple transactions giving rise to breaches across CBNA London's operations, involving activity across a number of business areas and functions. This includes payment processing, correspondent banking and account restrictions. OFSI's assessment is that many of the breaches arose from specific systems and controls issues and/or errors by CBNA London staff, or staff in the wider Citi group acting on its behalf. These issues arose in the context of the high volume of Russia-related sanctions designations following the invasion of Ukraine in 2022, which OFSI considers placed significant strain on the bank's alert handling and investigation processes. In particular, delays in the review and escalation of sanctions alerts, and some instances of human error, appear to have contributed to the breaches.

7. CBNA London voluntarily disclosed the majority of the breaches to OFSI, whereas some other breaches came to OFSI's attention by other means. CBNA London co-operated with OFSI's investigation and OFSI considered that CBNA London was eligible for a voluntary disclosure and co-operation discount of 20%.

8. OFSI issued CBNA London a Notice of Intention to impose a monetary penalty on 15 June 2026. OFSI and CBNA London agreed to enter formal settlement discussions on

29 June 2026, commencing 1 July 2026. Settlement was agreed on 11 August 2026.

BACKGROUND

9. CBNA London operates as the UK branch of Citibank, N.A., the US-headquartered global financial institution. CBNA London serves as a core wholesale bank in the UK and as a correspondent bank. Additionally, CBNA London is a key entity in the provision of cross-border payments, cash management and multicurrency accounts for transactions across its global payment network. It also facilitates market and securities activity by providing bank accounts and settlement services.

10. The breaches were varied and have been categorised within eight matters ("the Matters") relating to CBNA London processing payments, operating accounts or providing correspondent banking services in a manner that OFSI considers resulted in dealing with frozen funds, or funds being made available to or for the benefit of designated persons, contrary to UK financial sanctions. In one of the Matters, OFSI considers that CBNA London also breached its obligations to report frozen assets to OFSI as soon as practicable, which was aggravating to some of the breaches in that Matter.

11. OFSI imposed a monetary penalty on CBNA London because it was satisfied, on the balance of probabilities, that CBNA London breached prohibitions imposed by the relevant financial sanctions legislation. OFSI assessed the breaches together and imposed a single civil monetary penalty in respect of the total breaches, applying its case factor assessment across the whole case.

12. In total CBNA London processed 970 payments with a total cumulative value of £19,720,127.43, which OFSI considers to be breaches. There were a variety of different errors and failings that led to or related to the breaches, which are set out in more detail below.

13. In assessing this case, OFSI applied the guidance in place at the time of the decision to issue notice of an intended penalty, which was the 9 February 2026 version of the Financial Sanctions Enforcement and Monetary Penalties Guidance (Enforcement Guidance).

14. The breaches subject to penalty in this case occurred both before and after the strict liability amendments to PACA came into effect on 15 June 2022. This has been accounted for in OFSI's assessment of this case.

THE BREACHES

15. The breaches occurred across several components of CBNA London's business operations, including its corporate banking clients, correspondent banking and its role as Principal Paying Agent in respect of notes issued by an SPV on behalf of an entity whose beneficial owner became a designated person. The breach groups were as follows:

Corporate clients majority owned by designated persons:

16. CBNA London did not promptly restrict 24 commercial bank accounts held by 11 different companies owned or controlled by a designated Russian individual, resulting in the bank processing 242 payments with a total value of approximately £5.9 million which OFSI considers were in breach of regulation 11 (dealing with frozen funds) of the Russia Regulations. CBNA London also processed two payments valued in aggregate at over £600,000 from a company not owned or controlled by the designated Russian individual to a firm owned by that individual which OFSI considers was in breach of regulation 12 (making funds available) of the Russia Regulations. OFSI notes that £4.3 million of the approximately £5.9 million of transactions occurred within 24 hours of designation. The remaining breaches occurred over the course of several weeks. The issues which led to or related to the breaches were:

    a. Staff acting on behalf of CBNA London did not promptly identify and restrict the accounts of the relevant entities. This was because a backlog quickly emerged in the alert handling queues at the third level review stage due to large volumes of potential sanctions matches which required manual checking to resolve, resulting in some alerts remaining unadjudicated for several weeks;

    b. As a result of the operational pressures referenced above, staff within CBNA London and acting on its behalf did not promptly identify or action internal communications that would have alerted them to the fact that the accounts of some of the relevant entities had not been restricted; and

    c. Staff acting on behalf of CBNA London made an incorrect determination of ownership and control for one of the relevant entities, and a member of staff responsible for identifying accounts exposed to sanctions applied to designated majority owners, did not identify some of the relevant subsidiary companies associated with the designated person.

    d. To assist in managing the volume of alerts being generated at the time, CBNA London temporarily changed its guidance to sanctions staff in May 2022 such that it did not require them to request restrictions on an account which was subject to further investigation for sanctions exposure unless they had evidence of 50% or greater ownership of that entity by a designated person. Prior to this, staff were required to request restriction for all accounts potentially associated with designated persons (regardless of the percentage of the designated person’s interest or ownership in the entity) upon escalation to the team responsible for making a final decision. OFSI considers that in circumstances where there were delays in restricting accounts, the guidance change increased both the risk of accounts being left unrestricted and the duration.

17. CBNA London did not promptly restrict 32 commercial bank accounts held by 29 different entities owned or controlled by designated person PJSC Sovcomflot ("SCF"), resulting in the bank processing 328 transactions with a total value of approximately £5.4 million which OFSI considers were in breach of regulation 11 (dealing with frozen funds) of the Russia Regulations. The issues which led to or related to these breaches were:

   a. CBNA London's screening system perceived a material difference between the name of the designated person as it appeared in OFSI's consolidated list ("Sovcomflot") and in its own Know Your Customer ("KYC") records ("PAO Sovcomflot"). Specifically, due to the screening system calibration, the system did not account for the Russian corporate prefix "PAO" in conjunction with the term Sovcomflot, and so did not produce alerts despite its KYC records indicating exposure to "PAO Sovcomflot"; and

   b. The processes in place at the time for identifying and restricting accounts involved manual steps, which were subject to significant delay due to the operational strain experienced as described above.

18. CBNA London also debited internal charges from some of the commercial bank accounts held by entities owned or controlled by SCF and the entities owned or controlled by the Russian individual after those accounts were restricted, the relevant issues for which are set out below under "Internal charges".

19. There was a general licence in place during the period CBNA London processed the majority of the payments involving entities owned or controlled by SCF, but as the bank processed the payments before its sanctions compliance controls had restricted the relevant accounts, and no transaction alert was generated, no prior assessment of whether the general licence applied was conducted in relation to the payments. At OFSI's request, CBNA London conducted an exercise after the fact to contact counterparties to the payments requesting further information, as well as OFSI doing so in some cases, in order to assess whether any were permitted by the general licence. This ultimately assisted OFSI's assessment of these breaches but prolonged OFSI's investigation into the matter.

Internal charges:

20. CBNA London deducted its own fees and tax charges from the accounts of some designated Russian individuals and companies, as well as companies owned or controlled by them, in a manner which OFSI considers breached the Russia Regulations. The bank also corrected some payment errors in a manner which OFSI considers also breached the Russia Regulations. These payments were generally low value. The bank processed 177 transactions of this type with a total value of approximately £135,000 in breach of regulation 11 (dealing with frozen funds) of the Russia Regulations when performing debits and in breach of regulation 12 (making funds available) when performing the credits. The issues which led to or related to these breaches were:

a. Most of the transactions took place on accounts which were restricted pending confirmation of a true match on the client who held the relevant account. The type of restriction CBNA London applied to the accounts whilst that determination was pending prevented customer and third-party debits but not the deduction of its own internal charges;

b. The processes in place for identifying and restricting accounts involved manual steps, which were subject to significant delay even where affected entities were identified, due in part to significant numbers of sanctions alerts following new measures responding to Russia's invasion of Ukraine. The timelines for performing account segregation extended significantly beyond the bank's target, often by several weeks or months; and

c. CBNA London's account management system allowed for the bulk processing of corrections to interest payments (including negative interest) without flagging that sanctions restrictions were in place.

21. There was a general licence in place during the period CBNA London processed some of the internal charge breach payments which permitted banks to deduct certain fees associated with the routine holding or maintenance of frozen funds. However, as the relevant internal debits were processed without sanctions alerts being generated, the bank made no prior assessment of whether the general licence applied before processing the payments. CBNA London and OFSI performed a retrospective assessment of whether or not payments were permitted by the general licence.

Russia-related correspondent banking:

22. Between February and June 2022, CBNA London processed 19 payments to designated Russian financial institutions acting as correspondent banks. The designated correspondent banks in these payments were Alfa-Bank JSC, PJSC Gazprombank and Credit Bank of Moscow. The total value of these payments, which OFSI considers breached regulation 12 (making funds available) of the Russia Regulations, was approximately £26,000. During the same period, CBNA London also processed 106 payments with a total value of approximately £650,000, which OFSI considered relevant to its assessment of the case, but on the particular facts of the payments did not treat them as breaches of the prohibitions in the Russia Regulations as they occurred before the entry into force of the PACA strict liability regime. In those 106 other payments, another non-UK Citi entity, as opposed to CBNA London, selected the designated person correspondent bank during the process of creating the payment chain after CBNA London had processed the payments. The issues which led to the 19 breaches occurring were:

a. CBNA London used an automated payment processor which selected correspondent banks from an internal list depending on payment route. This internal list included Russian banks which subsequently became subject to UK financial sanctions. The internal list was not screened against sanctions lists at the time of the payments; and

b. CBNA London's payment processor was configured to screen information relating to a payment before correspondent banks were added automatically, and it was not configured to re-screen the full payment chain once correspondent banks had been added. As a result, designated Russian financial institutions could be added to the payment chain after screening, and where this occurred their identifying information was not subsequently screened before the payments were released.

23. Between 24 March and 6 April 2022 CBNA London acted as remitting bank or correspondent bank when processing 160 payments where the beneficiary bank was a designated Russian financial institution or an entity owned or controlled by them. The designated banks in these payments were Alfa-Bank, Gazprombank, Bank GBP International SA, Russian Agricultural Bank JSC, Amsterdam Trade Bank. A further five payments involving the Ural Bank for Reconstruction and Development were processed between 22 April and 22 May 2022. The total value of all of these payments, which OFSI considers breached regulation 12 (making funds available) of the Russia Regulations, was approximately £729,000. The issues which led to these breaches occurring were:

    a. Certain internal Citi list entries used for screening had not been manually enriched to include the Bank Identification Codes (BICs) of the relevant designated banks, or entities owned or controlled by them at the time these payments were processed. In each case, the only identifying information in the payment messages for those entities was the BIC, as opposed to the name of the entity which is common practice for such transactions and in accordance with normal SWIFT message procedures. BIC details were added to the relevant internal Citi list entries on 5 April 2022, but a human error meant that the BIC for Ural Bank for Reconstruction and Development was not added until later.

24. Between September and October 2022, CBNA London processed 14 payments acting as correspondent bank between companies owned or controlled by a designated Russian individual. The total value of these payments, which OFSI considers breached regulation 12 (making funds available) of the Russia Regulations, was approximately £4m. The issues which led to these breaches occurring were:

    a. Due to system configuration, payment information for these payments was screened before the full correspondent banking chain was created. In these 14 payments, it was CBNA London itself which was added as a correspondent bank after the payments were first screened, and staff acting on CBNA London's behalf did not identify and act on the fact that there was a UK nexus and a UK designated person involved in the payments before they were released.

25. Between August and October 2022, CBNA London processed, as intermediary bank, the return of six payments to designated Russian financial institutions as ultimate beneficiary banks. It processed four payments to Rosbank and two payments to Gazprombank. The total value of these payments, which OFSI considers breached

regulation 12 (making funds available) of the Russia Regulations, was approximately £1.2m. The issues which led to these breaches occurring were:

a. The payments involved "point to point" return payment instructions. CBNA London had received and screened the initial outbound payments, which were not breaches, but CBNA London was later instructed by the non-designated beneficiary bank, AO Citibank, to return the funds. CBNA London screened the return payment message which only included the next bank in the payment chain, which was not a designated person, and did not contain the ultimate beneficiary banks, which were designated persons; and

b. CBNA London did not make use of information in its possession at the time of the payments in the form of the payment messages for the outbound transactions. As a result, it did not identify that the ultimate beneficiaries were designated Russian banks.

26. There were general licences in place during the period CBNA London processed the majority of the Russia-related correspondent banking breach payments which permitted the winding down of transactions with designated Russian banks. However, as no sanctions compliance alert had been generated the bank made no prior assessment of whether the general licences applied before processing the payments. At OFSI's request, CBNA London conducted an exercise after the fact to contact counterparties to the payments requesting further information, as well as OFSI doing so in some cases, in order to assess whether any were permitted by the general licence. This ultimately assisted OFSI's assessment of these breaches but prolonged OFSI's investigation into the matter.

Alert mishandles:

27. In a series of unconnected breaches which occurred between March 2022 and February 2025, CBNA London processed 9 payments where an alert handler made an incorrect decision. The designated persons in these payments were PJSC VTB Bank, Bank Otkritie Financial Corporation PJSC, Gazprombank OAO which majority owned Bank GPB International SA, Credit Bank of Moscow, Evraz PLC, AFK Sistema (which wholly owned East-West United Bank SA) and one designated Russian individual. The total value of these payments was approximately £500,000. The issues which led to these breaches occurring were:

a. The alert handlers and other staff acting on behalf of CBNA London made errors including following guidance which related to sectoral sanctions, issuing conflicting or incorrect instructions to colleagues, or failing to follow the terms of a licence issued by OFSI. In the highest value transaction, CBNA London received a payment from a Russian bank, which was designated the following day. A number of alerts were subsequently generated and dispositioned without issue, however, when the final alert was dispositioned several months later, the alert handler misidentified the role of the designated person by mistaking the designated Russian bank as the beneficiary, when in fact it was the remitter, and in error rejected the payment back to the designated person.

Interest payment:

28. In November 2022, in its capacity as Principal Paying Agent ("PPA") for loan participation notes issued by an SPV owned or controlled by a person, which (after CBNA London's appointment) became a designated person, CBNA London received, via a correspondent bank, funds representing an interest payment intended for distribution to noteholders. In February 2023 it rejected these funds and returned them to the correspondent bank, which OFSI has determined thereby made funds available indirectly to a designated person. The value of this payment, which OFSI considers breached regulation 12 (making funds available) of the Russia Regulations, was approximately £1.5m.

29. The issues which led to this breach occurring were:

    a. An alert generated against the loan participation notes was identified but staff within CBNA London failed to realise that the company for whom it acted as PPA was owned or controlled by a designated person and returned the funds. This was because a member of staff had previously failed to follow the correct procedure, which would have been to escalate sanctions concerns related to the relevant entity to sanctions compliance colleagues;

    b. Staff responsible for administering and agreeing to the payment and staff elsewhere in the bank did not share information effectively between themselves, which had they done so would likely have prevented the breach from occurring.

GAC correspondent banking payments:

30. Between January and July 2025, CBNA London processed as correspondent bank 10 payments, nine of which OFSI considers were made for the benefit of an individual designated under the GAC Regulations and one of which was made between two companies owned or controlled by that individual. The total value of those payments, which OFSI considers breached regulation 13 (making funds available for benefit of designated person), was approximately £300,000. The issues which led to these breaches occurring were:

    a. CBNA London first became aware that the remitter may have been owned or controlled by a designated person via an internal money laundering alert on payments which were under investigation at the time the person became subject to an asset freeze. Investigations took several months, as CBNA London sought and obtained information from the remitting bank to confirm the ownership and control of the remitter, and ultimately led staff to escalate concerns to sanctions colleagues. The above referenced payments were processed while those investigations were ongoing.

    b. The initial sanctions escalation was made to the incorrect team and this was not identified; therefore the escalation was not redirected, resulting in the case being closed at that time with no further action.

CASE ASSESSMENT

31. OFSI takes several factors into account when determining how seriously to view a case ("the Case Factors"). Within those factors, OFSI makes an overall assessment of (i) breach severity and (ii) the conduct of the person who has breached.

32. Overall, OFSI determined that the severity of this case was High, and that conduct was Aggravating. OFSI concluded that this case warranted the highest rating within its seriousness framework (Level 4). In arriving at this determination, and with reference to the factors set out in the Enforcement Guidance, OFSI's assessment is that the aggravating factors were as follows.

Aggravating factors

33. The aggregate value of the breaches was very high, at approximately £19.7m. The breaches related to corporate clients majority owned by designated persons and Russia-related correspondent banking each involved totals of approximately £5.3m and £6 million, respectively. The interest payment associated with the loan participation notes of a designated person was also a high value individual payment at £1.5 million. The case also involved a very high volume of payments, including repeated lower-value transactions, which cumulatively reached significant totals (Case Factor B).

34. OFSI considered the strategic priority of the Russia sanctions regime to be an aggravating factor. The majority of the breaches related to Russia sanctions, which are a strategic priority for the UK's foreign policy objectives, particularly following Russia's illegal invasion of Ukraine (Case Factor C).

35. OFSI considered that the breaches caused sustained, material harm to the objectives of the relevant sanctions regimes. Whilst OFSI accepts that there was no intention on the part of CBNA London to undermine the aims of the relevant sanctions regimes, the breaches nevertheless enabled designated persons or entities owned or controlled by them to access funds, settle obligations, or continue business operations in a manner which significantly undermined the effectiveness of sanctions (Case Factor D).

36. OFSI does not consider that CBNA London intended to breach sanctions regulations although, in line with OFSI's policy on Case Factor E, OFSI does not consider the absence of intent to be mitigating. For some of the payments processed after 15 June 2022, OFSI considered that CBNA London's systems contained the necessary information to determine that processing the payments was in breach of sanctions, but that information was not properly disseminated or identified at the time. This meant that there were in some cases, missed opportunities to prevent funds being made available to or for the benefit of designated persons. For all of the breaches, OFSI considered that CBNA London should have known or suspected that its actions would result in a breach of financial sanctions, which is aggravating (Case Factor E).

37. Across the case, OFSI investigated and carefully considered CBNA London's awareness and management of financial sanctions risk, particularly as it applied to

UK financial sanctions in the lead up to, and aftermath of, Russia's full-scale invasion of Ukraine in February 2022. OFSI's investigation focussed on elements of CBNA London's knowledge of sanctions, the preparation work it conducted in anticipation of sanctions and its compliance systems and controls most relevant to the breaches. OFSI has determined that many of the breaches in this case arose from specific systems and controls issues. OFSI has assessed whether or not the systems and controls issues (such as the SCF screening issue or lack of screening of internal correspondent banking lists) were reasonably foreseeable and concluded that they were. This was either due to the knowledge held by the bank prior to the issues occurring, or because they reflected aspects of the design or configuration of relevant systems and controls that OFSI considers might have been identified sooner through further stress-testing or analysis in the period leading up to Russia's February 2022 invasion of Ukraine. While Citi undertook significant work to prepare for the onset of sanctions, noting CBNA London's elevated exposure to Russia sanctions risks, OFSI would have expected to see a greater level of detail specific to CBNA London's UK operations than was provided in response to OFSI's questions on how it prepared for potential new sanctions against Russia in the period leading up to the invasion (Case Factor F).

38. In the case of the 242 payments processed from accounts of a designated Russian individual, OFSI considered that an incorrect determination of ownership and control was an aggravating factor. This is because the conclusion of minority ownership was not a reasonable one to draw from the information available to CBNA London (Case Factor G).

39. Most of the breaches within each Matter involved a pattern of repeated, persistent or extended breaches sharing the same or a similar root cause. The payments involving the interest payment associated with the loan and the alert mishandles were notable exceptions to this, but OFSI considers that, overall, the repeated, persistent or extended nature of the breaches in this case was aggravating (Case Factor H).

40. As an additional aggravating factor in connection with the breaches related to internal charges only, OFSI considered it aggravating that CBNA London did not report frozen assets to OFSI as soon as practicable on 53 occasions, with a delay of more than six weeks in all of those cases and in 11 cases 518 days, with the average time between CBNA London having reasonable cause to suspect that it held frozen funds on behalf of a designated person and submitting the corresponding frozen asset report to OFSI being 274 days.

41. These factors were weighed against the mitigating factors in the case.

Mitigating factors

42. The breaches related to internal charges deducted from the accounts of designated persons were usually low in value, which was mitigating to that group of breaches (Case Factor B).

43. The breaches related to internal charges deducted from the accounts of designated persons were mitigated by the lower degree of harm they posed to the aims of the sanctions regime. This is because the internal charges did not result in funds being made available to designated persons, were of a type commonly licensed by OFSI and they derived no meaningful benefit from them (Case Factor D).

44. The interest payment and alert mishandles were mitigated by those matters not having been repeated, persistent or extended (Case Factor H).

45. As additional mitigating factors, OFSI noted that:

    a. Some of the payments were made shortly after a designated person became subject to an asset freeze. OFSI does not necessarily expect payments completed very close to the time of designation to be stopped by automated screening systems. Proximity to designation was strongly mitigating to the majority of the 244 breaches relating to the corporate clients majority owned by designated persons, where roughly £4.3m of the £5.9m total occurred within 24 hours. Nevertheless, these payments are included in the breach total because there were later further breaches of the same or similar nature.

    b. CBNA London undertook a programme of remediation to address the root causes identified in connection with the breaches. CBNA London also demonstrated openness in sharing its corrective action plans and additional information on the progress of its remediation with OFSI.

    c. Although not directly related to OFSI's investigation into the breaches, Citi's decision to withdraw from Russia reduces the risk of future breaches of the Russia Regulations occurring and aligns with the aims of the UK's sanctions regime, and is therefore somewhat mitigating.

46. OFSI recognises that the unprecedented size, scale and complexity of the sanctions measures introduced by the UK and its allies following Russia's invasion of Ukraine in 2022 created significant operational challenges for firms with exposure to Russia. While this context did not excuse the breaches, OFSI took it into account when assessing the case, particularly those breaches which occurred in early 2022 relating to sanctions screening, alert handling and investigation processes.

47. Other case factors were considered either not relevant, or on balance to be neither aggravating nor mitigating.

48. OFSI does not consider that CBNA London sought to circumvent sanctions in any of the matters (Case Factor A). However, in line with its published guidance, OFSI does not consider the absence of circumvention to be mitigating. This factor is not relevant to the case.

Overall assessment

49. In accordance with the Enforcement Guidance, and after considering both aggravating and mitigating factors, OFSI assessed this case overall to be Level 4.

50. OFSI does not consider there to have been any intent by CBNA London to breach sanctions. However, the errors and failings referred to above were, in aggregate, material and significant and they occurred across a wide range of business areas and systems within the bank. The overall severity of the case is high, and the conduct aggravating, with the issues relating to the corporate clients matter being particularly concerning to OFSI in light of the length of time which elapsed between designation and the relevant accounts being properly restricted. The aggregate value of the breaches in the case is very high, the case involved systems and controls issues that OFSI considers were aggravating as well as some missed opportunities to prevent breaches, and OFSI considers that they caused severe and lasting damage to the purposes of the sanctions regime. Taking all of these matters together, and assessing the relevant mitigating factors referenced above, OFSI therefore considers this case meets the criteria for Level 4.

MONETARY PENALTY

Permitted maximum penalty

51. The permitted statutory maximum for a monetary penalty is:

    1) In a case where the breach or failure relates to particular funds or economic resources and it is possible to estimate the value of the funds or economic resources, the greater of:

        a) £1,000,000, and

        b) 50% of the estimated value of the funds or resources.

    2) In any other case, £1,000,000.

52. In this case, the total value of the breaches was £19,720,127.43. The permitted maximum for a monetary penalty is therefore £9,860,063.72.

Baseline penalty

53. Within this maximum, OFSI decides what level of monetary penalty is reasonable and proportionate, based on its view of the seriousness of the case. OFSI's Enforcement Guidance states that a reasonable and proportionate baseline penalty amount for Level 4 cases should be at or above 75% of the statutory maximum.

54. Taking into account all the relevant circumstances of this case, OFSI considers that £7,888,050.97 is a reasonable and proportionate baseline penalty amount.

Voluntary Disclosure and Co-operation discount

55. OFSI will reduce the monetary penalty amount by up to 30% where a person has voluntarily self-reported breaches to OFSI in a prompt and complete manner, subsequently provided OFSI with a complete account of the circumstances of the breach, and thereafter cooperated with OFSI's investigation.

56. In this case, OFSI determined that CBNA London was entitled to a voluntary disclosure and co-operation discount of 20%. In reaching this view OFSI was particularly mindful of the following facts:

a. That CBNA London voluntarily disclosed all but two of the groups of breaches, but the two groups it did not voluntarily disclose had a significant total value. CBNA London only became aware of the breaches relating to SCF and the interest payment because OFSI wrote to it proactively which led to CBNA London conducting reviews that identified the full extent of the breaches. In the case of the interest payment, it is not clear to OFSI that CBNA London would have become aware were it not for OFSI raising questions, which is cause for concern. The total value of breaches considered to not be voluntarily disclosed was approximately £6.9m.

b. Of the matters which were voluntarily self-disclosed, two were not disclosed promptly when they arose in 2022. Due in part to an internal sanctions investigation ongoing at the bank, the 14 correspondent banking breaches between companies owned by a Russian individual were disclosed to OFSI approximately seven months after CBNA London first identified them as potential breaches, whilst some of the internal charge breaches were disclosed with a delay of approximately ten months. The total value of breaches voluntarily disclosed but which OFSI considers were not promptly disclosed was approximately £4m.

c. OFSI considers that some of the bank's initial disclosures in 2022 were materially incomplete and in the most serious examples, although it was not the bank's intention to do so, the disclosures contained some inaccurate information. This was the case for the breaches involving entities owned or controlled by SCF, where CBNA London's initial description of the cause did not reflect the full facts, which only came to light following scrutiny by OFSI in August 2025, three years after the breaches occurred and at a late stage in OFSI's investigation. CBNA London had also inadvertently provided some incorrect information in 2022 indicating that PAO Sovcomflot was its customer, when in fact it was not, which caused unnecessary and avoidable delays in OFSI obtaining the full facts of that case. Despite notifying OFSI promptly upon identifying the issue, OFSI considers that CBNA London provided a materially incomplete initial disclosure for the GAC correspondent banking payments, where it omitted a key contributory factor which only came to light on further questioning by OFSI. The bank also did not initially disclose a substantial number of the internal charge breaches because of an error in how it set the parameters for identifying those breaches.

d. The bank was unable to provide full information in the initial reports for some of the Russia-related correspondent banking breaches. This was because, at the time it processed the payments, no sanctions alerts were generated against the relevant payment and it had been unaware that they were prohibited by financial sanctions, and therefore had made no prior assessment of whether or not a payment was permitted by the general licences which were in force. This caused delays of several months to OFSI's investigation, as well as the expenditure of significant resource by OFSI to attempt to obtain information after the event.

e. Over the course of the investigation, CBNA London provided materially prompt and complete responses to OFSI's voluntary questions and committed at an early stage to answering all voluntary questions as best it could. The bank at times provided OFSI with documents and information beyond that requested which assisted OFSI's consideration of the case. The bank also voluntarily provided OFSI with regular updates on wider matters related to the winding down and sale of AO Citibank, and some transactions it judged did not engage sanctions but which involved Russian persons or entities and chose to disclose in the interests of full transparency.

f. CBNA London undertook a wide range of internal reviews and investigations into the breaches and provided OFSI with regular updates and disclosed the findings. Some of those investigations were proactive, others were carried out in response to requests by OFSI. OFSI wrote to CBNA London on 8th November 2022 asking for details of all remaining undisclosed matters, in response to which the bank sent a comprehensive summary on 25th November 2022 of all of the matters in respect of which it was then conducting reviews.

g. Throughout the investigation, CBNA London offered to hold calls with OFSI to discuss the breaches and provide further context and explanation. In the later stages of the investigation, CBNA London also made an unprompted offer to OFSI to hold technical briefings on a range of themes. The briefings were informative and contributed materially to OFSI's understanding of the breaches.

h. In a minority of cases, the bank's submissions contained inadvertent errors which contributed to delays in the investigation, and were often identified by OFSI rather than CBNA London. This included the submission on multiple separate occasions of transaction data across several breach groups which contained some duplicate payments, errors to the timestamps, the roles of the parties or sometimes data which was missing. These errors occurred in the context of the bank submitting a large quantity of other material and data which was correct, and the bank always promptly corrected the errors. However, the number of mistakes nevertheless caused delay to OFSI's investigation.

i. In two instances in the investigation, CBNA London inadvertently answered OFSI's questions in a manner OFSI considered omitted relevant context or information which could have assisted OFSI's understanding of the matters.

57. Having taken these matters into account, OFSI considers that the baseline penalty amount ought to be decreased by 20%.

Settlement discount

58. In accordance with the Enforcement Guidance, where settlement discussions between OFSI and the person on whom a penalty is to be imposed are successfully concluded within a 30-business day settlement period, OFSI will reduce the baseline penalty amount by 20%.

59. As OFSI and CBNA London reached agreement within the settlement period, OFSI has applied an additional 20% discount to the baseline penalty. Taken together, the total discount to the baseline penalty is 40%.

60. OFSI therefore imposed a monetary penalty of £4,732,830.58.

NOTES ON COMPLIANCE

61. This case offers important lessons for a wide range of firms and stakeholders with exposure to financial sanctions risks. Financial institutions in particular should study the matters set out above to assist in judgements as to whether their systems and processes could experience similar issues or give rise to sanctions risks which require addressing. Other firms which use automated systems or follow processes similar to those set out above, even if they are not financial institutions, should also consider these risks.

62. The case also demonstrates the importance of firms appropriately assessing their exposure to significant sanctions risks in advance, to a sufficiently detailed degree to understand where vulnerabilities may exist that could materialise or become more apparent when put under strain. Where a firm has elevated exposure to specific sanctions risks OFSI would expect to see evidence of sufficiently detailed prior analysis of potential vulnerabilities, especially in the context of rapidly increasing risk of new sanctions being introduced by the UK, as was the case for Russia sanctions in the period leading up to its illegal invasion of Ukraine in February 2022.

63. The case also involved general licences issued by OFSI, principally wind down general licences issued in relation to Russian financial institutions. General licences contain permissions and conditions designed to meet the purpose for which they were issued. Wind down general licences are issued to permit a person to wind down or divest from transactions involving the relevant designated person. They do not permit all payments related to a designated person irrespective of the purpose or for longer than is necessary to exit that relationship. Firms should note that OFSI expects parties to a transaction to take reasonable steps in advance to assure themselves that a general licence applies to that transaction, and to retain appropriate records of these efforts. OFSI considers that it is particularly important for entities operating accounts on behalf of a designated person to perform due diligence to ensure compliance with a general licence. As a general matter, where firms have exposure, they should ensure they are aware of the general licences relevant to their clients' operations, take appropriate advice as to the permissions of those licences, and maintain appropriate communications with their clients to remain satisfied of their compliance.

64. This case demonstrates the value that voluntary disclosure and co-operation with an OFSI investigation can provide. Voluntary self-reporting, provision of a complete account, and full ongoing co-operation can together result in a discount of up to 30% as part of OFSI's Voluntary Disclosure and Co-operation discount. To benefit from the full discount amount, firms should seek to make timely, comprehensive disclosures, providing OFSI with insight into the full facts of suspected breaches. Where full disclosure is not possible, a person should make an early disclosure with a subsequent fuller report submitted without unreasonable delay. Co-operation is expected to go above and beyond what the law requires and providing information beyond that explicitly requested. Firms are encouraged to provide information proactively where it may assist OFSI's investigation, including material not expressly requested but which is relevant to the issues under consideration. Although not relevant to this case, in potentially complex cases, firms may also wish to consider at an early stage whether to request access to the Early Account Scheme (EAS), as set out in Chapter 4 of the Enforcement Guidance.

NOTES ON SETTLEMENT

65. This case was resolved by means of settlement. OFSI regards settlement as a means to achieve timely and efficient enforcement outcomes. Resolving cases through settlement reduces the resource burden on OFSI and subjects that would otherwise be spent through the contested monetary penalty process. It can also result in messages about financial sanctions compliance being published sooner. OFSI therefore considers that it is in the public interest for matters to settle, and settle early, if possible.

66. Settlement is an agreement between OFSI and the subject of an enforcement action to resolve a monetary penalty case following a time-limited negotiation. As a condition of settlement, the subject must agree 1) to pay the penalty as imposed, and 2) to waive their rights to a ministerial review and to appeal OFSI's decision to the Upper Tribunal concerning the matters within the scope of the settlement. In return, the subject will have the opportunity as part of the negotiations to input into the summary of the case that will be published, and under the new scheme will also be entitled to a discount to the baseline monetary penalty (in addition to any other available discount) if they sign a settlement agreement within the applicable timeframe, usually 30 business days.

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