FINANCIAL CONDUCT AUTHORITY

12 Endeavour Square
London
E20 1JN

Tel: +44 (0)20 7066 1000
Fax: +44 (0)20 7066 1099
www.fca.org.uk

FINAL NOTICE

To: Starling Bank Limited

Reference Number: 730166

Address: London Fruit and Wool Exchange, 1 Duval Square, London, E1 6PW

Date: 27 September 2024

1. ACTION

1.1. For the reasons given in this Final Notice, the Authority hereby imposes on Starling Bank Limited ("Starling") a financial penalty of £28,959,426 pursuant to section 206 of the Act.

1.2. Starling agreed to resolve this matter and qualified for a 30% (stage 1) discount under the Authority's executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £40,959,426 on Starling.

2. SUMMARY OF REASONS

2.1. Following the opening of its first account in July 2016, Starling underwent exponential growth between 2016 and 2023, its customer base increasing to approximately 3.6 million in 2023 while its revenue increased to £452.8 million. Its financial crime controls, however, failed to keep pace with its growth.

2.2. The Authority identified serious concerns with Starling's anti-money laundering and financial sanctions framework during its review of financial crime controls at challenger banks in 2021. As a result of those concerns, Starling commenced an AML Enhancement Plan to address the FCA's concerns and voluntarily accepted a requirement from the Authority in September 2021 (the VREQ) not to open any new accounts for high or higher risk customers while it improved its AML control framework.

2.3. When the Authority imposes a requirement on a firm, it is imperative that the firm ensures it can comply with the terms of the requirement, including adapting its internal controls and monitoring its compliance with the requirement. Starling however failed to implement all of the underlying requirements and sub-requirements of the VREQ properly and did not adequately monitor its compliance with the terms of the VREQ following its imposition. As a result, over the Relevant Period, Starling opened 54,359 accounts for 49,183 high or higher-risk customers in breach of the terms of the VREQ.

2.4. Starling therefore contravened the VREQ which is a relevant requirement imposed under the Act.

2.5. Starling also identified in January 2023 that, since the implementation of its financial sanctions screening framework in 2017, its automated screening system had only been screening the names of new and existing customers against a fraction of the names on the Consolidated List. Although Starling took immediate steps to remediate this fault, its subsequent review of its financial sanctions framework identified wider systemic issues including Starling's assessment of its financial sanctions risk, policies and procedures, testing and calibration of screening systems, and a lack of MI regarding alert volumes and trends.

2.6. The Authority reminded regulated firms in February 2022 of the need to ensure that their financial sanctions systems and controls are robust to identify and prevent exposure to Designated Persons. In order to comply with their legal obligations not to conduct any prohibited activities with Designated Persons, firms should screen new customers and existing customers against the most recent Consolidated List to ensure they identify any sanctions exposure. Further, firms should ensure that they are not processing payments in breach of financial sanctions. Starling failed to ensure that its screening of customers and payments was sufficient to prevent this during the Relevant Period.

2.7. Principle 3 of the Authority's Principles for Businesses requires a firm to take reasonable steps to ensure that it has organised its affairs responsibly and effectively, with adequate risk management systems.

2.8. By failing to design, implement, and maintain adequate systems and controls to mitigate financial crime risks (in particular in relation to financial sanctions), Starling breached Principle 3.

2.9. The Authority hereby imposes on Starling a financial penalty of £28,959,426 pursuant to section 206 of the Act.

2.10. In determining the appropriate penalty, the Authority has taken into account that Starling has established programmes to remediate these breaches and to enhance its wider financial crime control framework. This has included:

(1) putting in place enhanced controls in respect of its monitoring and oversight of its compliance with the VREQ and in respect of its financial sanctions screening systems and controls. By the end of the Relevant Period, Starling had implemented effective control assurance activity to ensure ongoing compliance with the VREQ, and third-party testing of Starling's customer and payment sanctions screening systems had determined those systems to be operating effectively and efficiently as a result of Starling's remedial work;

(2) conducting a remediation exercise in respect of the customer accounts opened in contravention of the VREQ;

(3) carrying out historic financial sanctions screening reviews of its entire customer base and payments dating back to 2017; and

(4) significantly increasing its financial crime compliance resource.

2.11. Further, Starling has fully cooperated with the Authority's investigation, proactively offering and delivering presentations to the Authority and voluntarily providing important additional information.

2.12. The Authority hereby imposes on Starling a financial penalty of £28,959,426.

3. DEFINITIONS

3.1. The definitions below are used in this Notice:

"1LOD" means Starling's first line of defence (i.e. the business roles and functions directly engaged in operations, controls and risk management).

"2LOD" means Starling's second line of defence (i.e. compliance department and the risk functions which are responsible for overseeing the risk management framework).

"3LOD" means Starling's third line of defence (i.e. internal or external audit).

"the Act" means the Financial Services and Markets Act 2000.

"AML" means anti-money laundering.

"AML Enhancement Plan" means Starling's financial crime strategy from 2021 to 2022.

"the Authority" means the Financial Conduct Authority.

"CIFAS" means a fraud prevention service that operates two fraud prevention databases.

"Consolidated List" means a list maintained by OFSI containing Designated Persons.

"Consultancy Firm" means the independent compliance consultancy firm instructed by Starling in 2023 to conduct an independent review of its implementation of the VREQ.

"Designated Person" means an individual, entity or ship, listed under UK legislation as being subject to financial sanctions.

"DEPP" means the Authority's Decision Procedure and Penalties Manual, part of the Authority's Handbook of rules and guidance.

"Economic Crime Enhancement Plan" means Starling's financial crime risk strategy from 2023 to 2025.

"EG" means the Authority's Enforcement Guide.

"FCG" means the Authority's Financial Crime Guide.

"MI" means Management Information.

"MLRO" means Money Laundering Reporting Officer.

"NRA" means the UK's 2020 National Risk Assessment of money laundering and terrorist financing.

"OFSI" means the Office of Financial Sanctions Implementation, part of HM Treasury.

"PEP" means Politically Exposed Person.

"RCA" means Relative or Close Associate.

"PRA" means the Prudential Regulation Authority.

"the Relevant Period" means 1 December 2019 to 30 November 2023.

"SAR" means Suspicious Activity Report.

"Skilled Person" means the person appointed under section 166 of the Act following a requirement notice dated 28 May 2021.

"Starling" means Starling Bank Limited (FRN 730166).

"SYSC" means the part of the Authority's Handbook of rules and guidance which has the title Senior Management Arrangements, Systems and Controls.

"the Tribunal" means the Upper Tribunal (Tax and Chancery Chamber).

"VREQ" means the requirements imposed by the Authority on Starling under section 55L(5)(a) of the Act on 17 September 2021.

4. FACTS AND MATTERS

Background

4.1. Starling was authorised by the PRA on 12 July 2016 and since that date has been regulated by the Authority and the PRA. It offers a variety of services to customers, including the provision of personal current accounts, business banking, overdrafts, loans and money transfers.

4.2. Starling is a digital challenger bank. Challenger banks are a sub-sector of retail banks that aim to reduce the market concentration of traditional high street banks through the use of technology and more up-to-date IT systems. Digital banks have the following common features in their business models: they primarily offer

personal current accounts, they operate without a branch network, and they provide financial services through smartphone apps.

4.3. The Authority has identified challenger banks as an important part of the UK's retail banking sector. Specifically, the Authority has identified good practice in relation to their innovative use of technology to identify and verify customers at speed, allowing for quick and easy account openings. However, in its 2022 financial crime review (see paragraph 4.7 below for further details), the Authority found that the challenger bank sub-sector as a whole needed to do more in relation to their financial crime controls.

4.4. In the last few years, challenger banks have experienced significant growth both in their revenue and the numbers of customers opening accounts with them. In the case of Starling, its revenue increased from £13,000 in 2016 to £452.8 million in 2023, while its customer base grew from approximately 43,000 customers in 2017 to approximately 3.6 million in 2023. Further, the number of international or cross border transactions undertaken by Starling has increased substantially, including the number of inbound cross border payments rising from 385 in 2017 to 236,527 in 2020, and then to over 1 million in 2023.

4.5. When a financial institution undergoes such growth its systems and controls must also grow and adapt to ensure its continued compliance with the Authority's rules and Principles, and that they are fit for countering the risk that the firm might be used to further financial crime.

Authority's review of challenger banks financial crime controls

4.6. In December 2020, the NRA raised the risk that criminals may be attracted to the faster onboarding process offered by challenger banks when compared to traditional high street banks. The NRA identified that where challenger banks promote the ability to open accounts very quickly to attract customers, there is a risk that their due diligence is insufficient to identify high risk customers.

4.7. Following the identification of this serious risk, the Authority undertook a review of the financial crime controls at a sample of challenger banks during 2021. The purpose of this review was to identify the financial crime risks that challenger banks might be exposed to.

4.8. The Authority's review included six challenger retail banks, with a sample size of over 8 million customers. One of the challenger banks reviewed was Starling. The review of financial crime controls covered:

(1) governance and management information;

(2) policies and procedures;

(3) risk assessments;

(4) identification of high risk/sanctioned individuals or entities;

(5) due diligence and ongoing monitoring; and

(6) communication, training and awareness.

4.9. The findings of the review were published on 22 April 2022. The review stated that weaknesses found by the Authority created an environment for more significant risks of financial crime to occur both when customers are onboarded and throughout the customer journey. In summary, the Authority made multiple findings relating to how challenger banks manage their financial crime risk, including:

(1) financial crime control resources, processes and technology needed to be commensurate with a bank's expansion;

(2) challenger banks should apply a risk-based approach to AML controls and continuously ensure that their financial crime controls remain fit for purpose as their business develops and grows;

(3) there were weaknesses in customer due diligence, for example most challenger banks did not obtain details about customers' income and occupation;

(4) some challenger banks were not consistently applying enhanced due diligence and not documenting it as a formal procedure to apply in higher risk circumstances; and

(5) there was inadequate management of transaction monitoring alerts, including inconsistent or inadequate rationale for discounting alerts.

Authority's concerns with Starling's AML controls

4.10. In late 2020, the Authority identified several issues relating to Starling's AML and financial sanctions systems and controls, governance and oversight, and policy and processes in the course of its review of challenger banks' financial crime systems and controls. It wrote to Starling on 11 March 2021 setting out its wide-ranging

concerns and expressed concern that Starling had failed to adequately convey the significant issues identified by an internal audit report dated November 2018 on Starling's financial crime control framework to either Starling's Board or the Authority. While that internal audit report recognised a number of areas of good practice, it identified several significant gaps in Starling's financial crime procedures and controls and recommended that Starling address these within a year where practical.

4.11. The Authority in its feedback letter noted that Starling had grown rapidly in the past year and envisaged that this growth would continue. It stressed the importance of Starling ensuring that its financial crime systems and controls continue to develop so that they remained fit for purpose at all times.

4.12. Following receipt of the Authority's feedback letter, on 26 March 2021 Starling commenced an AML Enhancement Plan to address the Authority's concerns.

Skilled Person review and imposition of VREQ

4.13. As a result of the feedback letter, the Authority required Starling on 28 May 2021 to appoint the Skilled Person. The Skilled Person was instructed to test the adequacy of Starling's transaction monitoring and financial crime risk governance and oversight.

4.14. The Skilled Person's findings, in particular potential weaknesses in Starling's customer onboarding controls, increased the Authority's concerns about Starling's financial crime controls. At the request of the Authority, Starling voluntarily applied for requirements to be imposed upon how it carried out its business. The Authority imposed the VREQ on Starling's Part 4A permission on 17 September 2021.

4.15. The VREQ included the following requirement:

"*The Firm must not accept or process any new or additional account applications (whether for personal use, business use or otherwise) from new or existing customers that are:*

- *High risk, these include but are not limited to those which are cited as high risk by the Joint Money Laundering Steering Group (JMLSG) and those identified by the Firm;*
- *Customers or applicants which demonstrate higher risk financial crime characteristics* ***'higher risk persons'.***"

The VREQ included 20 sub-requirements defining specific activities and characteristics that should be considered higher risk and a further 6 associated requirements.

4.16. The purpose of the VREQ was to stop Starling onboarding any more high risk or higher risk customers (as defined by the VREQ) or opening new accounts for existing high risk or higher risk customers, in the absence of a sufficiently robust and effective financial crime control framework to manage the risk presented by these customers until it had sufficiently progressed its AML Enhancement Plan.

4.17. The VREQ has not been substantially varied since it was imposed and remains in place.

Breach of the VREQ

4.18. When a firm is subject to a requirement, it must correctly implement the necessary changes to its systems and controls to ensure that the terms of the requirement are met immediately and on an ongoing basis, until the requirement is varied or cancelled by the Authority.

4.19. Following the imposition of the VREQ, the firm introduced a series of controls to ensure compliance with its terms. These included:

(1) where a customer provided identification from certain jurisdictions, the onboarding journey would then move to a manual exception queue;

(2) PEPs and RCAs were subject to senior management and MLRO review and sign off;

(3) the system would only allow the onboarding of customers with United Kingdom standard addresses; and

(4) senior management and 2LOD review and approval was required for any customers where Starling discovered adverse media.

4.20. On 21 July 2022, Starling identified that a key financial crime risk control was not functioning correctly, resulting in new accounts being opened and services being provided for customers who had been previously exited for financial crime reasons. As these former customers fell within the VREQ's definition of high risk or higher risk persons, the opening of these new accounts breached the terms of the VREQ.

4.21. Starling resolved the issue with this financial crime control within a day and also undertook an impact and root cause analysis. Starling did not inform the Authority of this issue until the following month, on 24 August 2022. A couple of days later, on 26 August 2022, Starling notified the Authority that:

(1) It had breached the VREQ and explained the reasons for the breach: the financial crime risk control had not updated correctly, resulting in 294 customers that had previously been exited by Starling for financial crime reasons opening new accounts.

(2) Of these 294 customers, 161 had been previously subject to a SAR and 112 customers had either a full or partial match on CIFAS.

(3) Starling put in place additional controls following the discovery of this failure. Its 2LOD also commenced a review of Starling's compliance with the VREQ to identify any potential breaches and any areas for improvement in controls, oversight or assurance.

4.22. This 2LOD review of Starling's compliance with the VREQ subsequently became a workstream of the Economic Crime Enhancement Plan which launched on 17 October 2022 and superseded the AML Enhancement Plan. The objective of the Economic Crime Enhancement Plan is to develop Starling's financial crime risk management to a point where it meets industry best practice, including with respect to VREQ and financial sanctions screening compliance, and has involved significant financial investment to improve Starling's capability, structure and resources across its 1LOD and 2LOD. By November 2022, the 2LOD review had identified that an additional 309 accounts had been opened in breach of the terms of the VREQ. At this point, Starling elevated its financial crime risk rating to 'red', concluding that there was *'a heightened risk that the Bank could be used as a vehicle to further financial crime in addition to the risk of further regulatory action as a consequence of the reported breaches'*. Its risk assessment rating was based on the VREQ breach, and a backlog of high risk customer reviews and customer screening alerts.

4.23. Starling completed its 2LOD review of its compliance with the VREQ in December 2022. The review found that thousands of accounts had been opened by Starling in contravention of the VREQ and confirmed that, following its implementation of the VREQ on 17 September 2021, Starling had not put in place a formal monitoring programme to ensure that it had been meeting the VREQ's specific requirements.

4.24. In response to these findings, Starling put in place a remediation programme, which included, from 17 January 2023, an oversight programme of daily testing and assurance activity against the VREQ requirements. By 31 May 2023, Starling instituted automated daily controls to ensure its compliance with the VREQ.

External review of the breach of the VREQ

4.25. On 31 March 2023, the Authority wrote to Starling again in relation to its AML and financial sanctions control framework, and its implementation of the VREQ. The Authority recognised the significant investment made by Starling in its AML systems and controls and operational capacity to address the findings from the FCA's review in March 2021 and the subsequent Skilled Person's reports. However, it stated that the findings from Starling's 2LOD VREQ review and the volume of high-risk customers onboarded in breach of the VREQ without detection since September 2021 demonstrated that Starling did not fully recognise its regulatory obligations or apply the necessary rigour during implementation or through its oversight arrangements to ensure the controls relating to the VREQ were effective. The Authority also noted its disappointment that Starling did not immediately report the initial VREQ breaches to it, as well as the fact that Starling continued to report ongoing VREQ breaches, albeit at a much lower volume.

4.26. The Authority requested that Starling's Board carry out a 'lessons learned' review to assess the root causes of the weaknesses in the implementation of the VREQ and develop an action plan to respond to the findings.

4.27. As a result, Starling engaged the Consultancy Firm to carry out an independent review of its implementation of the VREQ. The Consultancy Firm conducted a review of Starling's governance, control framework and the roles and responsibilities of senior management surrounding the implementation of the VREQ.

4.28. The Consultancy Firm provided a report to Starling on 21 September 2023 which identified the following causes behind the breach of the VREQ:

(1) Starling's senior management as a whole lacked the experience and capability to effectively implement the VREQ, specifically:

(a) They lacked the required AML skills or experience. This resulted in an inadequate design of the financial crime VREQ risk management framework.

(b) They were inexperienced when dealing with significant regulatory changes. Starling's senior management lacked awareness of the impact of the VREQ and the seriousness of not complying with the VREQ.

(2) Starling's senior management failed to adequately oversee and monitor the day-to-day compliance with the VREQ:

(a) Starling failed to ensure that the oversight and responsibility for the implementation of the VREQ was delegated to an appropriate Senior Management Function holder. Several members of senior management at Starling had different understandings of whom at Starling had responsibility for the VREQ. This confusion resulted in there being no single person with sufficient authority and oversight to ensure the adequate implementation of the VREQ.

(b) Starling's senior management did not provide effective challenge and oversight of those responsible for the day-to-day implementation of the VREQ. There were also key failings in the communications between senior management and the staff responsible for the day-to-day implementation of the VREQ. In particular, the engineering teams – who were responsible for making the key changes to Starling's systems and controls to implement the VREQ – were not informed of the existence of the VREQ or the seriousness and potential consequences of not implementing the VREQ appropriately. Starling's 3LOD was unaware of the VREQ until late 2022.

(c) There was an absence of quality and consistently reported MI, with different committees receiving different information. This had the natural consequence of there being a lack of MI that the Board could assess and challenge. What MI was provided was sometimes not focussed on the adequacy of the implementation but rather how the VREQ could be reduced or removed. The poor quality and inconsistency of the reported MI meant that Starling was unable to conduct any meaningful challenge of the VREQ implementation process.

(3) The 1LOD, 2LOD and 3LOD functions were inadequate in their oversight of Starling's compliance with the VREQ:

(a) The financial crime function, which provided support and guidance to the executive function of Starling, was unable to perform its function adequately due to being under-resourced at the time of the VREQ implementation and during 2022 and therefore lacking key AML experience and capability.

(b) There was an absence or ineffective operation of controls required to implement and oversee the VREQ. Once the VREQ breach was discovered, some of the contraventions were identified as being repetitive. These repetitive contraventions of the VREQ could have been remediated if identified earlier. The VREQ contraventions were also caused by procedures not being followed or updated.

(c) The Consultancy Firm determined that documents outlining the roles, responsibilities and testing carried out by the 1LOD and 2LOD did not exist. It also found that Internal audit did not at the time robustly challenge the other two lines of defence, noting that Starling was in the midst of its AML Enhancement Plan whose primary objective was to grow and mature its financial crime risk management framework.

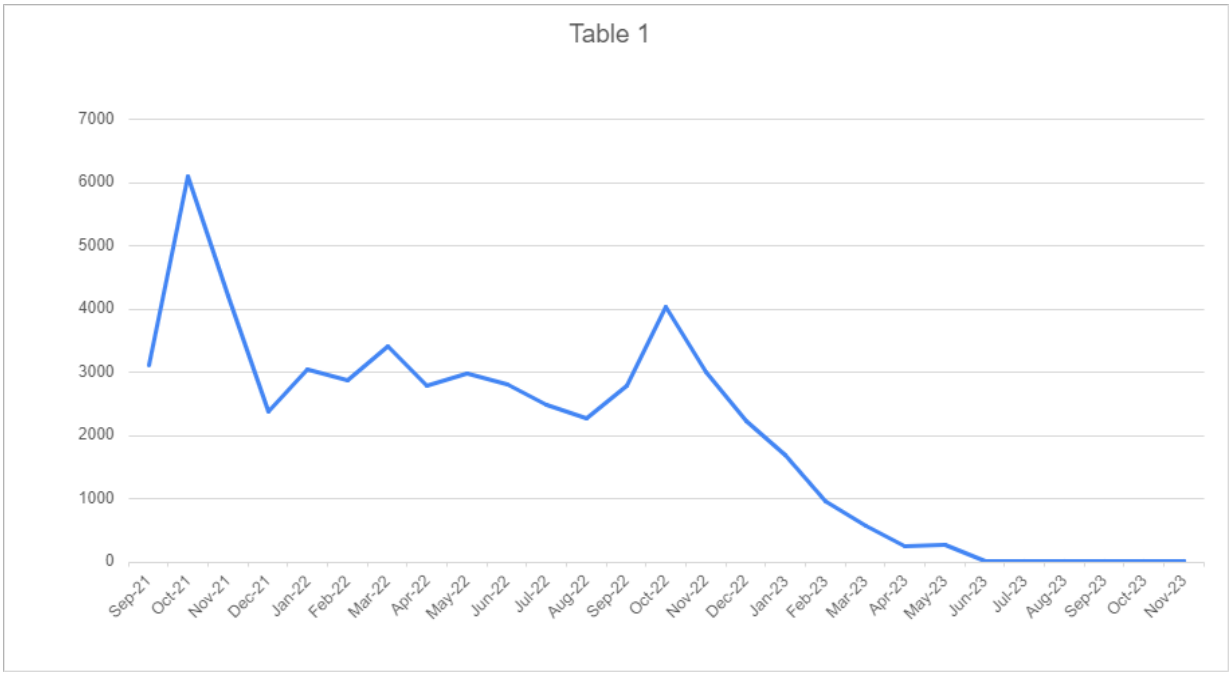
4.29. The Consultancy Firm's report also acknowledged that, as at 21 September 2023, Starling had taken various actions on its own initiative since concerns with VREQ compliance had first been identified, including improving the skills, experience, capabilities and resourcing of senior management and the 2LOD, the level of executive oversight and Board challenge, and the design of the financial crime VREQ risk control framework as part of the Economic Crime Enhancement Plan (albeit the report also acknowledged that the Consultancy Firm had not assessed the adequacy and appropriateness of these measures).

4.30. On 26 September 2023, Starling accepted all the findings in the Consultancy Firm's report and committed to correcting the failings identified, noting that all of the recommendations in relation to the VREQ were either already completed, in progress or scheduled for implementation.

Extent and frequency of VREQ contraventions

4.31. Between 17 September 2021 and the date of this Notice, Starling created 54,359 accounts of 49,183 high-risk or higher-risk customers in breach of the VREQ. Table 1 below indicates that the daily automated VREQ controls, which were introduced in January 2023 and fully implemented by 31 May 2023, resulted in a significant

decrease in the number of customers onboarded in contravention of the VREQ from that point forward (see paragraph 4.24 above):



4.32. In April 2024, Starling reported to the Authority their first month since the imposition of the VREQ where no high-risk customers were onboarded in contravention of the VREQ.

Overview of the UK financial sanctions regime

4.33. Financial sanctions are restrictions put in place by national governments or multilateral organisations that limit the provision of certain financial services or restrict access to financial markets, funds and economic resources in order to achieve a specific foreign policy or national security objective.

4.34. Financial sanctions are an important part of UK foreign policy and also support its national security. The UK's financial sanctions are imposed either by the UK government or by the United Nations (which requires member states to implement them through Resolutions passed by the UN Security Council).

4.35. Financial sanctions come in several forms, including targeted asset freezes which apply to Designated Persons, restricting their access to funds and economic resources.

4.36. All individuals and legal entities who are within or undertake activities within the UK's territory must comply with UK financial sanctions that are in force. Further, all UK nationals and legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

4.37. OFSI works to ensure that financial sanctions are properly understood, implemented and enforced in the UK. As part of its responsibility, OFSI maintains two public lists of those currently subject to financial sanctions, including the Consolidated List which details all Designated Persons. OFSI aims to update the Consolidated List within one working day of all new UN and UK listings coming into force in the UK, and within three working days for all other amendments.

4.38. Breaches of financial sanctions must be reported to OFSI at the earliest opportunity. The consequences of breaching a UK financial sanction can be serious, and OFSI has the power to impose monetary penalties for breaches and to refer cases to law enforcement agencies for investigation and potential prosecution.

4.39. While the Authority is not responsible for enforcing UK financial sanctions, its role is to ensure that the firms it supervises have adequate systems and controls to comply with the UK's financial sanctions regime.

Authority's concerns with Starling's financial sanctions controls

4.40. As noted in paragraph 4.10 above, the Authority was significantly concerned about Starling's financial sanctions systems and controls following its review of challenger banks in 2021. In its feedback letter to the firm dated 11 March 2021, the Authority stated that:

(1) Starling's financial sanctions policy stated that it screens customers and transactions against the sanctions lists issued by the UK, European Union, the UN and the US Department of the Treasury (OFAC), but that in practice Starling only screened its customers against the sanctions records for individuals who were known to reside or have links to the UK. Also, in contradiction of Starling's policy, the Authority noted that Starling was not screening its customers against sanctions records for individuals from other countries, including the United States of America, despite payments being made in US dollars.

(2) Starling accepted the risk that it could open an account for a sanctioned individual if other authorities were not aware that the individual had moved

to the UK, however Starling had provided limited rationale on why it was comfortable accepting this risk.

(3) Starling should update its financial sanctions policy in line with current business practices and assess whether it should be screening more than the UK Sanctions list.

4.41. In February 2022, the Authority wrote to thousands of regulated firms including retail banks. The purpose of the communication was to remind firms that their financial sanctions systems and controls should be robust, should be capable of being adapted in line with the recent changes made to the Russian sanctions regime, and should be appropriate to readily respond in the event of changes. This communication was sent to Starling on 24 February 2022 and noted in particular that Starling should ensure that:

(1) it screened new customers, payments and existing customers against the most recent version of the Consolidated List;

(2) its screening systems were effective, up-to-date and appropriate for the nature, size and risk of its business; and

(3) its senior management ensured there was adequate oversight and testing of Starling's relevant systems and controls to ensure they were appropriate at all times and to ensure Starling's compliance with its legal obligations under the amended Russia (Sanctions) (EU Exit) Regulations 2019.

4.42. In January 2023, Starling's 2LOD commenced a review of its screening of financial sanctions (called the "Sanctions Screening Review"), in which the 2LOD undertook a full end-to-end review of the bank's sanctions screening framework for both customer and payments screening.

4.43. The Sanctions Screening Review identified on 30 January 2023 that Starling's automated customer screening system had not produced any financial sanctions screening alerts for individual customers between 1 July 2022 and 30 January 2023. The lack of alerts had been caused by a system misconfiguration which affected the matching between the details of individual customers of the bank and individuals on relevant sanctions lists including the Consolidated List. This misconfiguration had existed since 20 July 2017 and resulted in customers or prospective customers only being screened against individuals on the Consolidated List with UK citizenship or UK residency during this period (i.e. 39 of the 3088 Designated Persons). This meant that there was a material risk that Designated Persons would have been able

to open accounts or, in the case of updates to the Consolidated List, continue to maintain accounts opened with Starling before February 2023. Starling identified that during the Relevant Period, at least one Designated Person had opened an account with them.

4.44. On 16 February 2023, Starling made a Principle 11 notification to the Authority that the bank's automated screening system had not produced any financial sanctions screening alerts for individual customers of Starling between 1 July 2022 and 30 January 2023. In the same notification, Starling also confirmed that it had already reconfigured and tested the customer screening system configuration on 10 February 2023, and recommenced live screening. It had also commenced an expedited customer back book screening review of Starling's current active customer base at the time (3.5 million customers) from 10 to 24 February 2023.

4.45. The customer back book screening review was completed on 24 February 2023 and generated approximately 48,000 alerts which were reviewed by financial crime operations.

4.46. The report of the Sanctions Screening Review identified that there were underlying failures in Starling's financial sanctions systems and controls including:

(1) Starling's risk assessment of financial sanctions was not sufficient to inform its risk decisions and the management of its financial sanctions risk. Starling had rated its sanctions risk as low and had failed to consider several high-risk factors such as payments from crypto-related platforms and multi-currency accounts.

(2) Starling's policies and procedures relating to financial sanctions screening were inadequate and required updating and enhancing, including updates in relation to the responsibilities of Starling's staff and reporting, testing and MI requirements. It was also identified that Starling lacked a standalone procedure for Sanctions screening alerts and instead possessed only a general procedure which did not provide any explanation as to what a screening alert was nor how to manage said alerts.

(3) Starling had no formal methodology or mechanism for the testing and calibration of its financial sanctions screening systems at or after implementation. The result of this was that it had no means to ensure that its sanctions screening process was functioning as required and that Starling

was complying with financial sanctions legislation. There was also no record of testing and calibration having been carried out.

(4) There was no operational MI relating to financial sanctions, this included alert volumes and trends which should have allowed Starling to monitor the effectiveness of both configurations and its overall financial sanction screening effectiveness.

(5) Concerns were raised in relation to Starling's governance of the financial sanctions screening. The review flagged that there appeared to be a '*capability gap*' at governance level in Starling in understanding sanctions compliance requirements. This was evidenced by an insufficient understanding surrounding the use of the Consolidated List and the risk parameters involved in financial sanctions screening. This was compounded by the fact that up until the first quarter of 2023 there were no 2LOD assurance reviews for sanctions screening and the 3LOD audit in relation to financial sanctions screening was delayed until the third quarter of 2023.

(6) Starling was screening its customers against the Consolidated List only once every 14 days. The 14-day period was a leftover metric from when Starling was a smaller institution and is not in keeping with current industry standards for similar financial institutions. The Sanctions Screening Review also identified that screening only occurred after a customer had been onboarded by Starling.

(7) Starling was not screening all of its cross border/international payments against the Consolidated List, despite such payments presenting a much higher financial sanctions risk than domestic payments.

(8) When screening payments against the Consolidated List, Starling was using a tool designed for customer screening and as such not designed to screen against payments.

(9) Lastly, the Sanctions Screening Review noted that Starling had been notified of issues with its financial sanctions screening processes in 2021, where an independent compliance consultancy found that Starling had not conducted frequent second line assurance monitoring of sanctions screening controls.

4.47. The final report of the Sanctions Screening Review was provided to Starling's senior management on 24 April 2023. Starling's senior management had already accepted the findings contained in a draft of the Sanctions Screening Review report earlier

in February 2023 and had started its remediation programme from then. Additionally, Starling agreed to make the necessary changes to address the issues and failings in its systems and controls identified in the Sanctions Screening Review. These improvements included:

(1) increasing its screening frequency for customers from once every 14 days to daily;

(2) the implementation of a new payments screening solution;

(3) updating the financial sanctions alert management system to ensure that previously raised matches with similar names or other details are not missed in the case of updates to sanctions lists;

(4) a review and redrafting of Starling's sanctions policy;

(5) creation of sanctions testing methodology to articulate responsibilities and testing requirements and the defining of a regular programme of configurations testing;

(6) third party testing of both the customer screening and payment screening systems;

(7) the designing of MI which monitors alert volumes and trends relating to sanctions, which is a critical indicator of the effectiveness of configurations and overall screening effectiveness;

(8) the introduction of governance and version control around lists used in the sanctions screening process and additional training for staff in relation to screening;

(9) the creation of a sanctions screening framework which captures all components of configuration management to ensure compliance with Starling's obligations under SYSC; and

(10) the creation of role specific training for Starling employees along with the review and enhancement of firm wide sanctions e-learning modules.

4.48. Third party testing of Starling's customer screening systems determined in November 2023 that those systems were operating at an effective and efficient capacity. The third party testing further concluded in March 2024 that Starling's payment screening systems were also operating at the same capacity.

4.49. As a result of Starling using the incorrect screening tool for the sanctions screening of payments (see paragraph 4.46(8) above), Starling commenced a review of historical payments on 22 May 2023. This review covered a total of 3,988,143 applicable payments processed between 24 May 2017 and 9 November 2023, including international/cross border transactions, which generated 795,712 alerts. The purpose of this review was to:

(1) identify, remediate, and report any payments Starling has processed in contravention of the applicable sanctions legislation;

(2) identify and remediate any accounts which have been involved in potential or confirmed sanctions breaches; and

(3) identify any customer links to Designated Persons, pre or post designation, to ensure a risk based approach is adopted for the monitoring and management of this population.

4.50. The review combined screening of the full payments back book against applicable sanctions lists with targeted screening of payments that were potentially associated with alerts identified through the systematic screening. The review was completed in September 2024 and identified a number of potential financial sanctions breaches. Starling reported the potential financial sanctions breaches to the relevant authorities.

5. FAILINGS

5.1. The regulatory provisions relevant to this Notice are referred to in Annex A.

Breach of the VREQ

5.2. The requirements in the VREQ were imposed by the Authority under section 55L(5)(a) of the Act. By virtue of section 204A of the Act, they are therefore 'relevant requirements' in respect of a contravention of which the Authority is entitled to take action.

5.3. On the basis of the facts and matters set out in paragraphs 4.19 to 4.23 and paragraphs 4.31 to 4.32 above, the Authority considers that Starling contravened relevant requirements imposed upon it, in that:

(1) The VREQ required that Starling "*must not accept or process any new or additional account applications (whether for personal use, business use or otherwise) from new or existing customers that are:*

- *high risk, these include, but are not limited to, those which are cited as high risk by the Joint Money Laundering Steering Group (JMLSG) and those identified by [Starling];*

- *customers or applicants which demonstrate higher risk financial crime characteristics '**higher risk persons**'."*

(2) The VREQ defined 'high risk' and 'higher risk' persons for the purposes of this requirement and included 20 sub-requirements and a further 6 associated requirements.

(3) Starling created 54,359 accounts of 49,183 high-risk or higher-risk customers during the Relevant Period in contravention of the requirements imposed on it in the VREQ (see paragraph 4.31 above).

Principle 3 breaches

5.4. Principle 3 of the FCA's Principles for Businesses requires that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

5.5. On the basis of the facts and matters in paragraphs 4.40 to 4.50, the Authority considers that Starling breached Principle 3 in the Relevant Period because it failed to take reasonable care to organise and control its systems and controls for managing the risk of financial crime (in particular in connection with financial sanctions) responsibly and effectively. In reaching this view, the Authority has taken account of the following:

(1) Starling's assessment of its financial sanctions risk was insufficient to inform its risk decisions and management of this risk (see paragraph 4.46(1) above);

(2) Starling's policies and procedures relating to financial sanctions were inadequate for purpose and required updating and enhancing (see paragraph 4.46(2) above);

(3) Starling did not test the effectiveness of the configuration of either its customer screening or its payments screening at or after implementation (being the implication of the matters in paragraph 4.46(3) above);

(4) There was no operational MI relating to alert volumes and trends which would have allowed Starling to monitor the effectiveness of configurations and overall screening effectiveness (see paragraph 4.46(4) above);

(5) Starling did not carry out any 2LOD assurance reviews of its financial sanctions screening or a 3LOD audit specifically for financial sanctions screening during the Relevant Period until Q1 and Q3 2023 respectively (see paragraph 4.46(5) above);

(6) Starling performed inadequate screening of customers and was screening them only once every 14 days (see paragraph 4.46(6) above);

(7) Starling did not screen all of its cross border/international payments against the Consolidated List (see paragraph 4.46(7) above);

(8) Starling used a tool designed for customer screening for its financial sanctions screening of payments (see paragraph 4.46(8) above); and

(9) between 20 July 2017 and 30 January 2023 Starling only screened against individuals on the Consolidated List with UK citizenship or UK residency (see paragraph 4.43 above).

6. SANCTION

6.1. The Authority's policy for imposing a financial penalty is set out in Chapter 6 of DEPP. In respect of conduct occurring on or after 6 March 2010, the Authority applies a five-step framework to determine the appropriate level of financial penalty. DEPP 6.5A sets out the details of the five-step framework that applies in respect of financial penalties imposed on firms.

Step 1: disgorgement

6.2. Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify this.

6.3. As explained in paragraph 4.31 above, Starling onboarded and/or provided services to 49,183 customers in contravention of the VREQ. The Authority considers that Starling derived the following financial benefit directly from these customers by way of interest income and fees and commission.

6.4. The financial benefit derived from these customers totalled £900,000. In accordance with DEPP 6.5A.1G, the Authority has charged interest on the Firm's benefit at 8% from 1 December 2023 to 27 September 2024, amounting to £59,426.

6.5. Step 1 is therefore £959,426.

Step 2: the seriousness of the breach

6.6. Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area. The Authority considers that the revenue generated by Starling is indicative of the harm or potential harm caused by its breach.

6.7. The Authority has therefore determined a figure based on a percentage of Starling's relevant revenue. Starling's relevant revenue is the revenue derived by Starling during the period of the breach. The period of Starling's breach was from 1 December 2019 to 30 November 2023. The Authority considers Starling's relevant revenue for this period to be £1,119,042,195.

6.8. In deciding on the percentage of the relevant revenue that forms the basis of the step 2 figure, the Authority considers the seriousness of the breach and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breach; the more serious the breach, the higher the level. For penalties imposed on firms there are the following five levels:

Level 1 – 0%

Level 2 – 5%

Level 3 – 10%

Level 4 – 15%

Level 5 – 20%

6.9. In assessing the seriousness level, the Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed

deliberately or recklessly. DEPP 6.5A.2G(11) lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factors to be relevant:

(1) the breaches revealed serious or systemic weaknesses in the firm's procedures or in the management systems or internal controls relating to all or part of the firm's business (DEPP 6.5A.2G(11)(b)); and

(2) the breaches created a significant risk that financial crime would be facilitated, occasioned or otherwise occur (DEPP 6.5A2G(11)(c)).

6.10. DEPP 6.5A.2G(12) lists factors likely to be considered 'level 1, 2 or 3 factors'. Of these, the Authority considers the following factors to be relevant:

(1) there was no or little risk of loss to consumers or other market users individually and in general (DEPP 6.5A.2G(12)(b)); and

(2) the breaches were committed negligently or inadvertently (DEPP 6.5A.2G (12)(e)).

6.11. Taking all of these factors into account, the Authority considers the seriousness of the breach to be level 4 and so the Step 2 figure is 15% of £1,119,042,195.

6.12. Pursuant to DEPP 6.5.3(3)G, the Authority may decrease the level of penalty arrived at after applying Step 2 of the framework if it considers that the penalty is disproportionately high for the breaches concerned. Notwithstanding the serious and long-running nature of Starling's breaches, the Authority considers that the level of penalty would nonetheless be disproportionate if it were not reduced and should be adjusted.

6.13. In order to achieve a penalty that (at Step 2) is proportionate to the breach, and having taken into account previous cases, the Step 2 figure is reduced to £40,000,000.

Step 3: aggravating and mitigating factors

6.14. Pursuant to DEPP 6.5A.3G, at Step 3 the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach.

6.15. The Authority considers that the following factor aggravates the Principle 3 breach:

(1) The Authority wrote to Starling on 24 February 2022 alongside thousands of other regulated firms to remind it of the importance of having robust systems and controls in place to ensure compliance with financial sanctions (DEPP 6.5A.3G(2)(l)).

6.16. The Authority considers that the following factors mitigate the breaches:

(1) Starling has established programmes to remediate its breaches and to enhance its wider financial crime control framework. This has included putting in place enhanced controls in respect of its monitoring and oversight of its compliance with the VREQ and in respect of its financial sanctions screening systems and controls, as well as significantly increasing its financial crime compliance resource; and

(2) Starling has fully co-operated with this investigation (including admitting and accepting the failings identified in the Consultancy Firm's report at paragraph 4.28 above), proactively offering and delivering presentations to the Authority on multiple occasions.

6.17. Having taken into account these factors, the Authority considers that the Step 2 figure should not be increased or decreased.

6.18. Step 3 is therefore £40,000,000.

Step 4: adjustment for deterrence

6.19. Pursuant to DEPP 6.5A.4G, if the Authority considers the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further or similar breaches, then the Authority may increase the penalty.

6.20. The Authority considers that the Step 3 figure of £40,000,000 represents a sufficient deterrent to Starling and others, and so has not increased the penalty at Step 4.

Step 5: settlement discount

6.21. Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement.

6.22. The Authority and Starling reached agreement at Stage 1 and so a 30% discount applies to the Step 4 figure.

6.23. Step 5 is therefore £28,000,000.

Proposed penalty

6.24. The Authority hereby imposes a total financial penalty of £28,959,426 on Starling for contravening the VREQ and breaching Principle 3.

7. PROCEDURAL MATTERS

7.1. This Notice is given to Starling under and in accordance with section 390 of the Act.

7.2. The following statutory rights are important.

Decision maker

7.3. The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.

Manner and time for payment

7.4. The financial penalty must be paid in full by 11 October 2024.

If the financial penalty is not paid

7.5. If all or any of the financial penalty is outstanding on 14 October 2024, the Authority may recover the outstanding amount as a debt owed by Starling and due to the Authority.

Publicity

7.6. Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the Authority must publish such information about the matter to which this notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

7.7. The Authority intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

Authority contacts

7.8. For more information concerning this matter generally, contact Daniel Telfer or Mark Lewis at the Authority (email: dan.telfer@fca.org.uk / mark.lewis2@fca.org.uk).

Kerralie Wallbridge

Head of Department

Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A

RELEVANT STATUTORY AND REGULATORY REQUIREMENTS

1. Relevant Statutory Provisions

The Financial Services and Markets Act 2000

1.1. In discharging its general functions, the Authority must, so far as reasonably possible, act in a way which is compatible with its strategic objective and advances one or more of its operational objectives (section 1B(1) of the Act). The Authority's strategic objective is ensuring that the relevant markets function well (section 1B of the Act). The Authority has three operational objectives (section 1B(3) of the Act).

1.2. The Authority's statutory objectives, set out in section 1B(3) of the Act, include the objective of the integrity objective which is protecting and enhancing the integrity of the UKs financial system. The integrity of the UK financial system includes it not being used for a purpose connected with financial crime.

1.3. Principally of the Authority's operational objectives, the integrity objective (section 1D of the Act), is relevant to this matter. Section 1D of the Act states:

"*The integrity objective is: protecting and enhancing the integrity of the UK financial system.*

The integrity of the UK financial system includes –

a) Its soundness, stability and resilience

b) its not being used for a purpose connected with financial crime,

c) its not being affected by contraventions by persons of Article 14 (prohibition of insider dealing and of unlawful disclosure of inside information) or Article 15 (prohibition of market manipulation) of the market abuse regulation,

d) the orderly operation of the financial markets, and

e) *the transparency of the price formation process in those markets.*"

1.4. Section 55L(5)(a) of the Act states:

"*The FCA may, on the application of an authorised person with a Part 4A permission-*

a) *Impose a new requirement*"

1.5. Section 204A of the Act states:

"1) The following definitions apply for the purposes of this Part.

2)'Relevant requirement' means a requirement imposed-

a) by or under this Act"

1.6. Section 206(1) of the Act states:

"*If the Authority considers that an authorised person has contravened a requirement imposed on him by or under this Act… it may impose on him a penalty, in respect of the contravention, of such amount as it considers appropriate.*"

The UK's financial sanctions regime

1.7. The Authority's Financial Crime Guide provides practical assistance and information for firms of all sizes and across all FCA-supervised sectors on actions they can take to counter the risk that they might be used to further financial crime.

1.8. Chapter 7 of the Financial Crime Guide concerns the UK's financial sanctions regime. It provides (by way of overview) that:

(1) Financial sanctions are restrictions put in place by the UK government or the multilateral organisations that limit the provision of certain financial services or restrict access to financial markets, funds and economic resources in order to achieve a specific foreign policy or national security objective.

(2) All individuals and legal entities who are within or undertake activities within the UK's territory must comply with the EU and UK financial sanctions that are in force. All UK nationals and UK legal entities established under UK law, including their branches, must also comply with UK financial sanctions that are in force, irrespective of where their activities take place.

(3) The Office of Financial Sanctions within the Treasury maintains a Consolidated List of financial sanctions targets designated by the United Nations, the European Union and the United Kingdom, which is available from its website.

1.9. The UK imposes financial sanctions by way of secondary legislation that are made pursuant to powers in the Sanctions and Anti-Money Laundering Act 2018. A

contravention of a financial sanction imposed under UK law constitutes a criminal offence.

2. Relevant Regulatory Requirements

2.1. The relevant regulatory provisions as they were in force during the Relevant Period are set out below.

Principles for Businesses

2.2. The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Authority's Handbook. They derive their authority from the Authority's rule-making powers set out in the Act. The relevant Principles are as follows.

2.3. Principle 3 provides:

"A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems."

Senior Management Arrangements, Systems and Controls ("SYSC")

2.4. SYSC 6.1.1R provides:

> "*A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that firm might be used to further financial crime.*"

2.5. For these purposes, the Authority's Handbook defines 'financial crime' as follows:

> "*(in accordance with section 1H of the Act) any kind of criminal conduct relating to money or to financial services or markets, including any offence involving:*
>
> *(a) fraud or dishonesty; or*
>
> *(b) misconduct in, or misuse of information relating to, a financial market; or*
>
> *c) handling the proceeds of crime; or*

d) the financing of terrorism;

in this definition, "offence" includes an act or omission which would be an offence if it had taken place in the United Kingdom."

DEPP

2.6. Chapter 6 of DEPP, which forms part of the Authority's Handbook, sets out the Authority's statement of policy with respect to the imposition and amount of financial penalties under the Act.

The Enforcement Guide

2.7. The Enforcement Guide sets out the Authority's approach to exercising its main enforcement powers under the Act.

2.8. Chapter 7 of the Enforcement Guide sets out the Authority's approach to exercising its power to impose a financial a penalty.