Office of the Complaints Commissioner
16 Old Queen Street
London SW1H 9HP

Tel: 020 7877 0019
E-mail: info@frccommissioner.org.uk
www.frccommissioner.org.uk

21 June 2024

Final report by the Complaints Commissioner

Complaint number 202300790

The complaint

1. You raised a complaint with my office on 27 February 2024 as, whilst the FCA upheld your complaint, you were not satisfied with the information it provided you with about the steps it will take to resolve the issues identified and with the lack of a timeframe for doing so. You also wanted to know how this situation arose.

What the complaint is about

2. You complained to the FCA on 24 January 2024 that on 17 January 2024 you received an email purportedly from a previous "principal user" at your firm, however, they did not send this email. You explained to the FCA that *"Upon investigation it is clear that the email was sent by an FCA system and not the previous Principal User's email address. It had been modified by a system to look like it wasn't sent by the FCA."*

3. You also raised concerns that the email was sent through Salesforce, a US headquartered company.

What the regulator decided

4. The FCA upheld your complaint and apologised *"for the spoof email you received when you changed the Principal User on Connect."* You were also told that *"the Technology team who confirmed that the system is working as expected and impersonating external email addresses is a business requirement."*

5. As a resolution for your complaint, the FCA proposed to "*to only allow emails from the FCA domain (@fca.org.uk) to be used to send out emails"*, although it could not tell you when this change might be implemented.

6. In relation to your concerns about Salesforce, the FCA informed *"you that data storage is in the UK, even though the headquarters is in the US and that [the FCA] use Salesforce for customer relationship and case management."* You were provided with the IP address used to support this statement.

Why you are unhappy with the regulator's decision

7. You are not satisfied with the FCA's answer as you *"want[ed] the FCA to explain why they impersonated a personal email address (**Element one)** and promise to stop doing it within a reasonable timeframe - certainly within 3 months" (**Element two**),* as *"For the FCA to continue "impersonating external email addresses" is completely unacceptable."*

My analysis

Element one

8. You were told by the FCA in its Decision Letter dated 15 February 2024 that its system *"impersonating external email addresses is a business requirement"*. The letter did not go into any detail to explain what this meant or why this requirement was implemented.

9. However, you were then sent an email on 25 March 2024, which stated *"I would like to clarify that impersonating users is not part of our process and clearly the system was not working as anticipated."*

10. I was concerned about the fact that the area that implemented this "business requirement" seems to have done it in error, not realising that the FCA spoofing email addresses of regulated firms can never be a legitimate business requirement and there were no processes in place to prevent this from happening. The enquiries from the Complaints Team in relation to your complaint were not sufficient to make the area reconsider the position, further intervention from another team was required. As a result, the

Complaints Team were given the wrong information (that spoofing firm email addresses was a business requirement), which they passed onto you.

11. The answer given to you about how and why the spoofing happened was incomplete and ultimately, incorrect. For these reasons, I **uphold** this element of your complaint.

12. Based on the internal communications I had seen, it appeared that the FCA dealt with this issue, but I **asked it to provide an update** about what measures it now has in place to prevent such "requirements" being implemented in error, which clearly was the case here.

13. The FCA's response to my preliminary report stated that a new process involving different steps and technical teams to prevent things going wrong in a similar way was implemented in July 2021 (the 2021 process). Whilst the response stated the various stages involved in the 2021 process, I was not given any detail as to what these actually entailed; therefore it was not possible to determine whether these appear reasonable or not.

14. Furthermore, the FCA's response raised additional questions as to how long it had actually been spoofing email addresses of firms without noticing this was happening. As a result, I made additional enquiries with the FCA to gain a better understanding of how long this rouge practice was effective and whether the 2021 process would in fact help to prevent the occurrence of a similar issue.

15. The FCA's additional response to my follow-up query provided clarity but did not alleviate my concerns. The code that caused the system to spoof firm email addresses was deployed at some point before July 2021. However, as the FCA's internal systems changed around this time, it is not possible to determine when exactly this happened. In any event, there was a process in place that erroneously spoofed firm email addresses for over three years without the FCA realising this was a problem.

16. The FCA fixed the issue relatively fast once the problem had been identified, as set out below in Element two. However, I remain concerned that whilst there are technical safeguards and processes in place as of 2021, it is not clear to me that other checks are in place to ensure that a change, even if technically

sound, does not cause other problems or create cyber security and other risks or beach data protection legislation, as an example.

17. My concerns around the lack of sufficient processes to prevent unintended consequences of changes made to the FCA's systems etc. remain, even in light of the additional information provided by the FCA. This is because it was an FCA lead product architect who stated in February 2024, in response to this complaint, that *"the system is working as expected and spoofing external email addresses is a business requirement"*. In my view this is clear indication that whilst the technical side of the process may well be taken care of, there appears to be a gap in understanding that implementing a code or technical change which runs fine can have wider implications and pose a number of risks both to the FCA and to the users of its systems. The governance forum appears to be limited to the review of technical issues, not inclusive of wider considerations and does not appear to routinely involve second line reviews for example.

18. The FCA's comments about the size of the team developing the platform and the magnitude and complexity of the work are noted and understood. But it is precisely due to these factors that there should be closer co-operation between the technical teams and others who can support them with a review of the implications of proposed changes from other relevant points of view.

19. As such, I **recommend** that the FCA carries out a review of its processes applicable to its development and/ or technical teams to ensure that not only are they robust from a technical point of view, but that they are compliant with all relevant laws and security standards and do not create problems in other areas, be that cyber security, data protection or any other.

Element two

20. Under this Element I will consider your worry that the FCA potentially might not implement the "fix" or take too long to do so. Having reviewed the complaint file, it is clear that the FCA had taken your notification seriously and quickly took steps to rectify the issues identified. This was achieved through implementing the "fix" set out in paragraph 5 above, as suggested in the FCA's Decision Letter.

21. This is evidenced by the fact that, following the Decision letter you were sent the email of 25 March 2024, informing you that *"[the Complaints Team] have received a confirmation this morning that the fix had happened on Friday night and is now on live environment.* In this email the FCA also thanked you for raising this issue and helping it improve its processes.

22. The FCA responded, in my view, quickly and efficiently. Within two months of you raising the complaint, it resolved the problem. As such, I **do not uphold** this element of your complaint.

My decision

23. This is my final report. I uphold Element one of your complaint and recommend that the FCA reviews and updates its processes to include a wider group of people able to comment on all potential implications of a technical change.

24. I do not uphold Element two of your complaint as the FCA deployed the fix to the problem relatively quickly once the issues were recognised, as it told you it would.

Rachel Kent
Complaints Commissioner
21 June 2024