Administrative sanction of 9 October 2025 for non-compliance with professional obligations related to anti-money laundering / counter financing of terrorism

Luxembourg, 6 January 2026

Administrative decision

On 19 May 2025, the CSSF imposed an administrative fine amounting to EUR 185,000 (one hundred and eighty five thousand) on Rakuten Europe Bank S.A. (the "**Bank**"), authorised as credit institution in accordance with the provisions of Article 2 of the Law of 5 April 1993 on the financial sector, as amended, representing approximately one percent (1%) of its total annual turnover as of 31 December 2022, adjusted for the purpose of the calculation.

Legal framework/motivation

The administrative fine was imposed by the CSSF pursuant to the provisions of Article 2-1(1) of the Law of 12 November 2004 on the fight against money laundering and terrorist financing, as amended (the "**AML/CFT Law**"), read in conjunction with the provisions of Article 8-4(1), (2)(f) and (3)(a) of the AML/CFT Law for non-compliance with anti-money laundering / counter-financing of terrorism ("**AML/CFT**") professional obligations.

In order to determine the type of administrative sanction and its amount, the CSSF duly took into account all the information at its disposal and all the legal and factual elements set out and discussed, including those presented by the Bank during the contradictory phase of the non-contentious administrative procedure as well as the gravity and duration of the breaches existing at the time of the on-site inspection, and the financial situation of the Bank, in accordance with the provisions of Article 8-5(1) of the **AML/CFT Law**.

The CSSF has also considered the limited scope of the on-site inspection as well as the fact that the Bank had acknowledged the detected breaches, provided a general action plan and that it had confirmed to the CSSF that it had initiated corrective measures during and after the on-site inspection in order to remedy these breaches.

The professional obligations in relation to which the breaches were observed are namely quoted in the relevant provisions of:

(i) the **AML/CFT Law**;
(ii) the Grand-ducal Regulation of 1 February 2010 ("**AML/CFT Grand-ducal Regulation**") providing details on certain provisions of the AML/CFT Law, as amended; and

Commission de Surveillance du Secteur Financier

(iii) CSSF Regulation No 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing, as amended ("**CSSF Regulation No 12-02**"), which constitutes an implementing measure of the AML/CFT Law;

in accordance with the provisions applicable at the time of the on-site inspection.

Legal bases for the publication

This publication is made on a nominative basis in accordance with the provisions of Article 8-6(1) of the AML/CFT Law, pursuant to which the CSSF carried out an assessment in concreto, also taking into account the observations and arguments of the person concerned and the proportionality of the nominative publication, and ensured that such nominative publication of names did not jeopardise the stability of the financial markets or an ongoing investigation.

Context and major cases of non-compliance with the professional obligations identified

This administrative sanction is the result of an on-site inspection carried out by the CSSF on the Bank between February 2023 and November 2023 covering the AML/CFT framework, and more specifically the corrective actions taken by the Bank in response to the breaches sanctioned by another European national competent authority, as well as on the controls regarding the countering of terrorism financing. The inspection performed by this European national competent authority, and which took place in 2019, was part of the review of the Bank's AML/CFT framework relative to its provision of services through persons established in its territory. During its on-site inspection, the CSSF identified significant instances of non-compliance by the Bank with its professional obligations in relation to AML/CFT. Several similar breaches had already been identified by the other European national competent authority in 2020, although, according to the information provided by the Bank to the CSSF, corrective measures seemed to have been implemented. The breaches mainly concerned the following points:

- The Bank had not implemented an adequate transaction monitoring system. The scenarios included in the monitoring tool were not kept up to date (for example, the list of accounts considered by the Bank to require special monitoring was several years old) and did not cover all transactions. In addition, the Bank was no longer able to configure these scenarios in a relevant manner due to a loss of knowledge of the tool following staff departures in the IT and Compliance departments, as well as the use of a version of the tool that was no longer maintained/supported by the supplier. Although some of these violations had already been identified by the other European national competent authority, the Bank had still not implemented the required corrective measures four years after the inspection carried out by that authority. The project to replace the transaction monitoring tool had in fact not been completed due to repeated implementation delays, and the compensatory controls put in place proved to be insufficient. In addition, the technical implementation of certain transaction monitoring scenarios was incorrect (for example, the threshold applied in

practice in one scenario was not the one defined in the functional specifications) and the configuration of the rules was not sufficiently formalised. These elements constitute a breach of Article 3(2)(d) and (7) of the AML/CFT Law, of Article 1(3) of the AML/CFT Grand-ducal Regulation and of Articles 32 and 39(1) and (2) of CSSF Regulation No 12-02, emphasizing the obligation to pay special attention to transactions involving unusually high amounts and unusual transaction patterns, through a monitoring system covering all transactions. Furthermore, given its inadequate monitoring system, the Bank had failed to comply with Article 4(1) of the AML/CFT Law which requires professionals to implement controls to effectively mitigate and manage the risks of money laundering and terrorism financing ("**ML/TF**").
The CSSF also noted significant delays in the processing of alerts generated by the transaction monitoring tool: approximately 9% of alerts were closed more than 2 months after being created. The other European national competent authority had already noted a delay in the processing of these alerts and the Bank had increased human resources in order to process the alerts identified by this authority; nevertheless, these resources were not sufficiently sustainable, and some new alerts accumulated and remained pending at the time of the on-site inspection conducted by the CSSF. Such processing delays constitute a breach of Article 39(5) of CSSF Regulation No 12-02 which emphasizes the obligation to take the necessary measures rapidly when a suspicious activity or transaction is identified.

- The CSSF also found that the Bank had accumulated significant and recurring delays in processing alerts relating to customer screening against lists of persons subject to restrictive measures in financial matters, lists of politically exposed persons ("**PEP**") and the detection of persons subject to adverse media. At the time of the on-site inspection, the Bank had several thousand alerts awaiting review, including dozens relating to restrictive measures in financial matters or relating to terrorism. While the other European national competent authority had already identified a delay in the processing of similar alerts, it appears that the corrective measures put in place by the Bank were insufficient.

  These delays constitute a breach of Article 3(2)(d) of the AML/CFT Law and of Article 33(1) of CSSF Regulation No 12-02, as the Bank was unable to apply "without delay" potential restrictive measures in financial matters. The delay in processing PEP alerts (and thus the lack of detection of these persons) also prevented the application of enhanced due diligence measures, if applicable, which constitutes a breach of Article 3-2(4)(a) of the AML/CFT Law, Article 3(4) of the AML/CFT Grand-ducal Regulation and of Article 30(1) of CSSF Regulation No 12-02.

  Alerts concerning adverse media about certain business relationships being analysed late by the Bank, it also breached Article 39(5) of CSSF Regulation No 12-02 requiring that the monitoring system enables the necessary measures to be taken rapidly where elements that could reasonably indicate the presence of suspicious behavior or suspicious activity impacting the Bank are identified.

- At the time of the on-site inspection, although the Bank had identified potential ML/TF indicators for 44 customer files, in some cases it filed suspicious activity reports with the Financial Intelligence Unit ("**FIU**") several weeks late. The Bank subsequently clarified that it had been able to dispel doubts about some of these business relationships, but this nevertheless constituted a violation of the obligation to inform the FIU "without delay" in the event of suspected ML/TF, as provided for in Article 5(1)(a) of the AML/CFT Law. These delays in reporting suspicions were likely to allow the persons concerned to continue to engage in potentially illegal activities.

  The CSSF also noted that for a customer identified by the name screening system as having had his assets frozen in France due to his involvement in acts of terrorism, the Bank had taken more than six months to review the alert and had closed it as the person was no longer on the list of persons subject to restrictive measures in financial matters at the time of the review, and did not file a suspicious activity report to the FIU. The CSSF nevertheless considers that the activity of the customer, as well as its presence on the list, suggesting potential ties to terrorism activities, should have led the Bank to file a suspicious activity report to the FIU and thus constitutes a breach of Article 5(1)(a) of the AML/CFT Law.

- The Bank was unable to demonstrate that its automated controls on customers subject to simplified due diligence measures were functioning properly. The on-site inspection showed that, for several customers subject to simplified due diligence measures, the automated controls failed to identify instances where thresholds, beyond which the application of simplified due diligence measures was no longer permitted, had been exceeded. Consequently, the Bank did not comply with Article 3-1(4) and Article 4(1) of the AML/CFT Law, as well Article 2 of the AML/CFT Grand-ducal Regulation which require professionals to ensure compliance with the conditions for applying simplified due diligence measures in all circumstances. Regular testing of the proper functioning of automated controls, as well as their formalisation, are essential elements of the compliance framework.

- The CSSF also noted that when the Bank assessed the ML/TF risk of its customers, it did not take into account the country of residence of beneficial owners and persons purporting to act on behalf of or for a customer. During its inspection four years ago, the other European national competent authority had already identified a similar issue for which the Bank had defined a technical solution, but for which the implementation was significantly delayed. This constitutes a breach of Article 3-2(1) and (2) of the AML/CFT Law, Article 3(1) of the AML/CFT Grand-ducal Regulation and of Article 39(1) of CSSF Regulation No 12-02. Consequently, the CSSF identified several examples of customers for which the ML/TF risk was wrongly assessed and for which the risk assessment made by the Bank was too low to ensure the application of an appropriate level of due diligence. Indeed, in the case of a legal entity, the risk associated with the country of domicile can indeed often be drastically different from the risk associated with the country of residence of the beneficial owner or proxy; thus, all risks associated with the countries in question must be taken into account in order to correctly assess the ML/TF risk of a business relationship.