

Administrative sanction of 28 July 2025 for non-compliance with professional obligations related to “anti-money laundering / counter financing of terrorism”

Luxembourg, 02 December 2025

Administrative decision

On 28 July 2025, the CSSF imposed a reprimand on an entity (the “**Bank**”) authorised as a credit institution in accordance with Article 2 of the Law of 5 April 1993 on the financial sector, as amended.

Legal framework/motivation

This reprimand was imposed by the CSSF pursuant to Article 2-1(1) of the amended Law of 12 November 2004 on the fight against money-laundering and terrorist financing (the “**AML/CFT Law**”) read in conjunction with the provisions of Article 8-4(1) and (2)(b) 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, 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, in accordance with the provisions of Article 8-5(1) of the AML/CFT Law. In this context, the CSSF has notably taken into account the significant changes made to the Bank’s governance which have a substantial and appropriate impact on the risk culture in relation to AML/CFT in accordance with the requirements laid down in Article 5 (1a) of the Law of 5 April 1993 on the financial sector, as amended.

The CSSF has also considered the fact that the Bank has acknowledged the detected breaches and duly informed the CSSF it completed corrective measures in order to remedy these breaches after the on-site inspection.

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 amended Grand-ducal Regulation of 1 February 2010 (the “**AML/CFT Grand-ducal Regulation**”), providing details on certain provisions of the AML/CFT Law,
- (iii) the Law of 19 December 2020 on the implementation of restrictive measures in financial matters (the “**Law of 19 December 2020**”), and

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

in their version applicable at the time of the on-site inspection.

Legal bases for the publication

This publication is made on an anonymous basis in accordance with the provisions of Article 8-6(1), second indent letter (b) of the AML/CFT Law.

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

This sanction is the result of an on-site inspection carried out by the CSSF on the Bank between 7 September 2021 and 12 July 2023 covering the AML/CFT framework. During the on-site inspection, the CSSF identified breaches to the AML/CFT professional obligations applicable to the Bank which related in particular to the following points:

- The CSSF identified that a limited number of customers had been anonymised in a database which resulted in these customers not being subject to the ongoing name screening controls [i.e. controls, as foreseen by the Bank, to detect persons, entities or groups subject to restrictive measures in financial matters, political exposed persons (“**PEP(s)**”) and persons subject to adverse media]. Such omission constitutes a breach of Articles 4(3) of the AML/CFT Law and 39(2) of CSSF Regulation No 12-02 that require the Bank to have a complete customer database. The Bank was therefore not fully able to respond promptly to a request from the competent authorities asking whether it had a business relationship with a specific person. Furthermore, since these customers were not subject to name screening controls, the Bank could have had, without knowing it, customers who were PEPs or subject to restrictive measures; it therefore constitutes a breach of Articles 3(2)(d) of the AML/CFT Law, 33(1) and 39(1) of CSSF Regulation No 12-02 which require the Bank to be able to identify, without delay, persons subject to restrictive measures in financial matters and it also constitutes a breach of Articles 3-2(4) of the AML/CFT Law, 3(4) of the AML/CFT Grand-ducal Regulation and 30(1) of CSSF Regulation No 12-02 which require the Bank to be able to identify and to apply enhanced due diligence measures to PEPs. It should be noted that, once this error had been identified, the Bank performed a manual name screening control on all customers wrongly anonymised, which produced no positive hits against financial sanction lists.

The CSSF further noted inconsistent, incomplete and/or incorrect data in the customer database, in particular regarding nationalities or countries of residence. We noted that the Bank had self-identified the lack of completeness of customer information and launched an initiative to remediate the issue, even though the CSSF noted the initiative was not performed in a timely manner and the initiative did not address all data quality issues

identified. Such lack of data completeness and such inconsistencies constitute a breach of Articles 3(2)(a) & (d) and 4(3) of the AML/CFT Law, 16(1) and 39(1) & (2) of CSSF Regulation No 12-02. Indeed, it is important to have comprehensive and reliable customer data in order to accurately assess their Money Laundering / Terrorist Financing (“**ML/TF**”) risk level and to implement appropriate monitoring measures.

- Malfunctions were also observed in the name screening system (i.e. technical “bugs”) and in the processing of alerts. They resulted in the Bank informing with delay the appropriate authorities as for the presence of customers subject to financial sanctions. These instances constitute a breach of Articles 3 and 6, first paragraph of the Law of 19 December 2020 and of Articles 33(1) & (2) and 39(1) & (2) of CSSF Regulation No 12-02, since these articles emphasise the need to inform competent authorities “without delay” when persons subject to restrictive financial measures in financial matters are identified.

The CSSF furthermore noted that the Bank did not systematically report to the Financial Intelligence Unit (“**FIU**”) refused business relationships where the reason for refusal was a potential suspicion of money laundering, an associated predicate offence (such as fraud) or terrorist financing. The majority of such refusals were automatic rejections by the system due for example to a potential name screening hit and there was no analysis of whether such rejections should have been reported to the relevant competent authority. It was noted that the Bank contacted the FIU during the on-site inspection to further clarify requirements and ensured reporting was changed accordingly. Nonetheless, the CSSF considers that this constitutes a breach of Articles 5(1)(a) of the AML/CFT Law, 11(2) and 48(1) of CSSF Regulation No 12-02 as these articles require the Bank to inform the FIU promptly when they know, suspect or have reasonable grounds to suspect money laundering, an associated predicate offence or terrorist financing. Such reporting is however not possible if automated rejections are not being analysed.

The CSSF equally noted a lack of reporting of fraud cases (e.g. falsified documents) to the FIU. Due to a wrong understanding of the requirements of the FIU, the Bank did not consider that such cases were required to be reported to the FIU, even when in instances, the CSSF noted that the Bank was in contact with other law enforcement agencies. The CSSF considers that this equally constitutes a breach of Article 5(1)(a) of the AML/CFT Law.

- The CSSF noted shortcomings with regards to the risk-based approach applied by the Bank, particularly given that several ML/TF risk factors and variables were not considered in the customer risk assessment. Examples of risk factors, that the CSSF considered relevant but that were not or not sufficiently considered, were risk factors related to customer’s profession and/or source of wealth, customer’s residence and nationality, the risks associated with persons that have power of attorney and the delivery channels of the Bank’s products and services. For example, the CSSF identified cases of high-net-worth individuals residing or having connections with high-risk countries but where the Bank’s risk assessment was not elevated enough to ensure appropriate due diligence.

Equally, the CSSF noted that on an ongoing basis the customer risk assessment was not being kept up to date in timely and consistent manner. Indeed, a reassessment of the ML/TF risk of the customers was carried out annually, even though important risk factors could be identified during the year. Furthermore, this reassessment was delayed by a largely manual process.

The CSSF considers that the above observations constitute a breach of Article 3(2a) of the AML/CFT Law which requires the Bank to assess the ML/TF risk of its customers and Article 5(1) of CSSF Regulation No 12-02 which specifies that this risk assessment notably also includes the “*proxy*” (e.g. person with power of attorney). This equally constitutes a breach of Articles 3-2(1) and (2) of the AML/CFT Law, 3(1) of the AML/CFT Grand-ducal Regulation and 31(1) of CSSF Regulation No 12-02 which specify that the Bank has to apply enhanced due diligence measures on business relationships from high-risk countries, within the meaning of Article 1(30) of the AML/CFT Law, and transactions involving high-risk countries. With regards to the ongoing due diligence obligation, this furthermore constitutes a breach of Article 5(4) of CSSF Regulation 12-02 that requires the Bank to keep account of the development of risk during its monitoring of its business relationships and consequently adapt its risk assessment when there are new risk factors or the risk factors change.

These breaches were considered serious since the Bank had not deployed sufficient resources at the time of the on-site inspection to develop a fully automated reassessment system, despite it has a significant number of customers.

- The CSSF noted that the transaction monitoring did not monitor all the factors listed in Articles 3(2)(d) & (7) of the AML/CFT Law, 1(3) of the AML/CFT Grand-ducal Regulation, and 32(1) & (2) and 39(1) & (5) of CSSF Regulation No 12-02, consistently across its services and products. These articles read together require the Bank to perform transaction monitoring that considers the ML/TF risk of its customers, the behaviour of its customers and to identify and monitor unusual or large transactions. Even though the Bank was found to have mitigating controls in place that could indirectly identify such transactions in certain instances, the CSSF did not consider this sufficient as it did not guarantee systematic monitoring of the factors listed in the above articles. The CSSF further noted that the monitoring was only performed using semi-automated reports run and reviewed manually on a monthly basis while the level of daily transactions was considerable. The CSSF did not consider this sufficient to comply with Article 39(2) of CSSF Regulation 12-02 which requires such system to be automated, unless it could be proven that automation was not required in view of the volumes monitored and with its paragraph (5) requiring to implement a supervisory system that allows the Bank to be able to take measures rapidly when suspicious activity is identified.

The CSSF further noted that some transaction monitoring rules/scenarios implemented via the above mentioned semi-automated reports were not implemented in line with the functional specifications required by Compliance, meaning that what the Bank described as being monitored in its policies and procedures was not in line with the monitoring implemented in practice. The CSSF hence considers the Bank was not able to comply with

Articles 3(2)(d) and (7) of the AML/CFT Law, 1(3) of the AML/CFT Grand-ducal Regulation, 32(1) and 39(1) & (2) of CSSF Regulation No 12-02.

All these shortcomings related to the transaction monitoring process, both in the design of the scenarios and in their implementation, prevented the Bank to detect abnormal or unusual transactions, even though such transactions are likely to constitute indicators of money laundering or terrorist financing.