

Sanctions and suspicious activity reporting:

A comprehensive guide to avoiding common pitfalls

The sheer volume and dynamism of professionals' reporting obligations can be confounding. When authorities' main focus is international financial sanctions, it is essential to understand the when, how and to whom of reporting.

According to the Financial Intelligence Unit's (FIU) most recent statistics,⁽¹⁾ professionals generated 44,519 suspicious activity/transaction reports (SAR/STR) in 2023. Despite this significant figure, the Commission de Surveillance du Secteur Financier's (CSSF) on-site inspections continue to uncover failed or delayed reporting cases, representing a large share of the administrative sanctions related to anti-money laundering and counter-terrorism financing (AML/CTF) imposed since 2022.

While the detection and immediate reporting of suspicious activity or transactions is essential, the quantity of reports is less significant if they fall short of regulatory authorities' standards. The Wolfsberg Group's *Statement on Effective Monitoring for Suspicious Activity* states, "The Group does not believe that the value being derived from the (constantly increasing) volume of SARs/STRs is contributing proportionately to effective outcomes in the fight against financial crime".⁽²⁾

By understanding Luxembourg's money-laundering (ML), terrorism-financing (TF) and sanction reporting requirements and adhering to recognized guidelines, professionals can meet both the spirit and the letter of the law.

In this context, professionals should also prepare for the upcoming obligations of the EU's new AML/CTF package.



Understanding Luxembourg's fundamental reporting obligations

Professionals subject to the Law of 12 November 2004 on the fight against money laundering and terrorist financing must report any relevant ML/TF suspicions as well as international sanction breaches.

Common pitfalls

Practical advice for effective reporting

Professionals face a multitude of challenges when identifying and reporting suspicious behaviors, including:

- The innovative techniques criminals employ, which leverage changing technology and geopolitical shifts;
- The international or cross-border nature of ML/TF;
- The rapid execution of instant payments; and
- The involvement of third persons and intermediaries.

While no blueprint exists for crafting a perfect report, certain steps can help professionals elevate the quality of their reporting.

Each employee should be able to detect and prevent illicit activities, especially those with client-facing roles, including identifying potential warning signs and key indicators of suspicious activities or



transactions. Therefore, AML/CTF training plans must ensure that staff at all levels can recognize red flags, and are well-versed in the company's internal processes to efficiently and accurately escalate any concerns to the compliance function. Given the continual evolution of financial crime methods, these training plans should be regularly updated.

As most professionals have already implemented the necessary processes and culture for logging suspicious behavior, they should focus on improving the quality of the reports submitted to the FIU.

- While criminal offenses do not need to be qualified, **reports should include a clear and exhaustive outline** of the issues at play, business relationships, and the basis for suspicion. Entities must also select accurate indicators within goAML.
- **Relevant supporting documents should be appended to the reports**, such as the corroboration of transactions and source of wealth, documents considered forged, negative media reports identified, email exchanges with counterparties, and tax memorandums.
- **Data embedded in the reports must be exhaustive, accurate and structured.** Consequently, it should include a structure chart and transactions which follow the FIU's STR format guidelines.

Merely identifying a **negative media** article about a counterparty



involved in a transaction **does not automatically necessitate FIU reporting.** Instead, it should initiate a comprehensive and well-documented relationship evaluation to reveal any ML/TF risk that may require an FIU report. In turn, the report should reflect this evaluation's outcome, such as further details on the origin of funds linked to the negative media article.

Should professionals report sanction breaches to the FIU?

While the FIU is not responsible for enforcing sanction regimes, any attempt to circumvent sanctions is an ML predicate offense under the Luxembourg criminal code. Therefore, any suspicion of a Luxembourg sanction regime violation should be reported to the FIU. These suspicions could correlate with other offenses like corruption, tax fraud or forgery, such as providing false documentation to conceal a sanctioned individual as the beneficial owner.

Under the sanction regimes of other jurisdictions, detecting a breach could also be regarded as an **indicator of elevated ML/TF risk.** These detections should trigger an extensive review of the business relationship, potentially resulting in a SAR being submitted to the FIU.

The FIU has repeatedly clarified that they do not seek reports that



only concern sanctions without any related suspicious activity.

Anticipating the impacts of the upcoming AML/CTF Regulation and sixth AML/CTF Directive

Financial institutions that carry out transactions can struggle to manage their decision-making processes post-reporting or post-freezing orders. Thankfully, the EU's recently enacted AML/CTF package, which includes the sixth AML/CTF Directive ("AMLD6") and the AML/CTF Regulation ("AMLR"), is set to alleviate these challenges. Published in the Official Journal of the European Union on 19 June 2024, this legislative package clarifies the obligations regarding suspicion reporting and the FIU's investigatory authority.

The AMLR will be applicable in July 2027 and AMLD6 must be implemented into national laws by July 2027, with some requirements to be implemented by July 2025 and 2026.

The AML/CTF package sheds light on the timelines regarding temporarily suspended transactions due to ML/TF suspicions. Professionals will be able to execute the transaction in question if they:

- Have assessed its associated risks; and
- Have not received any contradic-

tory directives from the FIU within three working days of the report submission date.⁽¹⁰⁾

The AMLR requires Member States to set a maximum period of no more than 10 working days for which the FIU is authorized to suspend a transaction.⁽¹¹⁾

Regarding FIU requests, the Luxembourg FIU's guidelines clarify that standard requests require a response within a fortnight, requests marked "urgent" within a week, and "very urgent" within 24 hours.

In comparison, the AMLR requires professionals to reply to FIU information requests within five working days and allows FIUs to shorten this deadline, possibly to less than 24 hours, which would amplify professionals' already significant compliance burdens.⁽¹²⁾

Conclusion

Navigating the ever-changing landscape of AML/CTF legislation, regulations and guidelines demands a deep understanding and seamless execution of reporting obligations along with a commitment to the quality of the reports submitted to the FIU and the Ministry of Finance.

To fully comply with their reporting obligations, professionals must be able to detect persons subject to restrictive financial measures or ML/TF suspicions. The guidance of the Wolfsberg Group and the CSSF can help professionals implement adequate internal controls to detect sanctions and other ML/TF indicators.

The upcoming AML/CTF package changes will require professionals to proactively improve their analysis methods and reaction speeds to FIU or Ministry of Finance requests. In doing so, the industry fortifies its defenses against illicit activities, reinforces the integrity of its financial institutions, and contributes to a secure global community.

Nicolas MARINIER, Partner
Marie-Astrid DUPUY, Director
Andreas SCHMITT, Senior Manager
Jeanne BARREAU, Manager

Deloitte Luxembourg

Reporting requirements	FIU	Ministry of Finance
Reporting obligations and scope	In line with CSSF Regulation No 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing ("RCSF 12-02"), professionals must implement adequate internal procedures to detect and report suspicious activity or transactions to the compliance function. The function must retain the decision in writing regardless of whether a SAR/STR is sent to the FIU. ⁽³⁾ When the suspicion is confirmed, the reporting must be done without delay by using the appropriate reporting category available in goAML, the FIU's dedicated tool.	Professionals must implement adequate internal procedures to immediately detect persons subject to restrictive measures in financial matters.
	A transaction is suspicious when a professional knows, suspects, or has reasonable grounds to suspect that ML, an associated predicate offense or TF is being committed or has been committed or attempted, particularly regarding the person concerned, its development, the origin of the funds, and the operation's purpose, nature and procedure.	Screening must be performed every time sanction lists are updated. In practice, the market performs daily screenings. Even when professionals rely on service providers for the provision of sanction lists and their integration into the screening tool, they are still responsible for these lists exhaustiveness and update, as well as the accurate integration into the tool.
	This means no evidence of ML, an associated predicate offense or TF is required when reporting a suspicion. Instead, all that is needed are the circumstances that make this hypothesis likely.	The Law of 19 December 2020 on the implementation of restrictive measures in financial matters, together with the Grand-ducal Regulation of 14 November 2022, detail the implementation of restrictive measures in financial matters for Luxembourg. Any professional discovering a UN or EU sanction violation must report the enforcement of these sanctions to the Ministry of Finance. ⁽⁵⁾
Reporting timeframe to authority	Please keep in mind that professionals should send this information to both the FIU and the CSSF (parallel reporting) only if the SAR/STR's subject is a professional under the CSSF's supervision or a member of its management, or if the information reported is likely to have a more material impact on the financial sector. ⁽⁴⁾	Notably, this reporting requirement is not about conveying suspicion but confirming an actual infringement and implementing the freezing order. In these scenarios, the report is made by emailing the Ministry and including the relevant authority in copy (cc). This is either the CSSF for CSSF-supervised entities or the Commissariat aux Assurances (CAA) for insurance sector matters. The restrictive measures list and guidelines are also published on the Ministry of Finance's website (https://mfin.gouvernement.lu/).
Post-reporting obligations	The obligation to report suspicions "without delay" as per RCSF 12-02 means the filing process should occur as soon as the suspicious activity/transaction is brought to attention.	The authority expects the professional to identify any restrictive measures within one business day. However, the requirement to implement and report restrictive measures must be done "without delay" . ⁽⁶⁾
	Although professionals tend to exclude any counterparty subjected to a SAR/STR from their risk appetite, it is not mandatory to terminate existing business relationships once a suspicious activity or transaction has been identified and filed. However, if a professional concludes that a SAR/STR must be submitted for an existing business relationship, this relationship must be subject to specific enhanced due diligence measures, which must be described in the professional's internal policies and procedures. ⁽⁷⁾ Unless expressly authorized by the FIU, professionals are prohibited from revealing a suspicious report submission. The restriction applies to both the reported individual and any third parties.	Professionals must follow the Ministry of Finance's instructions and apply enhanced due diligence measures on the concerned counterparty.
	This "no-tipping off" rule is crucial to the investigation's integrity. It applies to the intention of and the actual filing of reports, as well as FIU investigations and information requests. However, communications to authorized entities like law enforcement or within the same group ⁽⁸⁾ are exceptions to this rule.	
	On the monitoring side, the Wolfsberg Group's statement discusses measuring the effectiveness of transaction monitoring programs, which are currently focused on quantity rather than quality. ⁽⁹⁾ Major focal points include: <ul style="list-style-type: none">- Developing a risk-based "monitoring for suspicious activity" program that provides highly useful information;- Improving the analytics used for detection; and- Optimizing case management systems and leveraging external data sources.	
	The Wolfsberg Group reiterates that the best indicator of SAR/STR quality and usefulness is feedback from authorities, which provides information to professionals about their decision on a filed SAR/STR. Professionals should not only use this feedback to determine whether to continue or close the business relationship, but also consider it an indicator of the filed report's relevance.	

1) Financial Intelligence Unit, *Rapport d'activité de la Cellule de renseignement financier* 2023, July 2024.
2) The Wolfsberg Group, *The Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity*, July 2024.
3) Article 48(2) of RCSF 12-02.
4) Article 33(2) of RCSF 12-02.
5) Article 6(1) of the Law of 19 December 2020 on the implementation of restrictive measures in financial matters.
6) Articles 1 and 2 of the Grand-ducal Regulation 14 November 2022 providing details on the Law of 19 December 2020 on the implementation of restrictive measures in financial matters.
7) Article 48(2) of RCSF 12-02.
8) Article 73(3) of the upcoming Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and Article 38(5) of RCSF 12-02.
9) The Wolfsberg Group, *The Wolfsberg Group Statement on Effective Monitoring for Suspicious Activity*.
10) Article 71(1) of the Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
11) Article 24 of the Directive of the European Parliament and of the Council on the mechanisms to be put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849.
12) Article 69(1) of the Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.