BASEL INSTITUTE ON GOVERNANCE

the Wolfsberg Group

Reporting suspicious crypto activity

Bridging supervisory expectations and operational realities



Basel Institute on Governance
Steinenring 60 | 4051 Basel, Switzerland | +41 61 205 55 11
www.baselgovernance.org | info@baselgovernance.org

Associated Institute of the University of Basel

Table of contents

Executive summary 3

1 Introduction 6

2 What constitutes a useful and actionable STR/SAR? 6

3 Effectiveness, quality and defensive reporting 8

4 Data quality and structured reporting 9

5 Blockchain analytics: Value, limitations and practical challenges 10

6 The limits of evidencing and tracing historical cryptoasset activity 12

7 Public-private and private-to-private cooperation 14

Conclusion 16

Key terms 17

Executive summary

This report summarises discussions at "Crypto STRs in practice: bridging supervisory expectations and operational realities", a breakout session organised by the Wolfsberg Group and the Basel Institute on Governance at the 2026 Global Conference on Criminal Finances and Cryptoassets.

This workshop brought together supervisors, FIUs, financial institutions and cryptoasset service providers to discuss the practical challenges of crypto-related suspicious transaction and activity reporting (STR/SAR) and how its effectiveness can be improved.

The discussions highlighted eight recurring considerations that participants regarded as relevant to improving the effectiveness of suspicious crypto activity reporting. Their application remains subject to the applicable legal and regulatory framework and to reporting entities' risk-based assessments.

1. **Judge STRs/SARs by their intelligence value, not their volume**. A good report is one that competent authorities can act on. Large volumes of reports that contain limited contextual or intelligence value may place pressure on both reporting entities and authorities and make prioritisation more difficult. Improving report quality can help authorities identify and analyse the most relevant information, while recognising that reports of limited apparent value in isolation may become significant when combined with other information.
2. **Alerts and red flags are only a starting point**. Red flags, alerts and risk scores are a starting point for analysis, not a reason to file. Reporting entities should use professional judgement and report when the information supports a genuine suspicion. Reporting simply to avoid criticism, or because questions remain open, adds little value.
3. **Explain the reasoning behind the suspicion**. The most valuable reports give a clear narrative: why the activity is suspicious, what was reviewed, what steps were taken and how the evidence led to the conclusion. Relevant context matters more than including every piece of available information.
4. **Get the data right and make it machine-readable**. Accurate identifiers, complete transaction data and structured formats such as XML allow FIUs to link reports, including across borders. These formats should cover all relevant persons, entities, transactions and accounts, including cryptoasset accounts. A report of limited value on its own can become significant when combined with information held elsewhere.
5. **Use blockchain analytics alongside other sources**. There was broad agreement that these tools should support, rather than replace, human analysis and decision-making. The tools are valuable, but attribution can be incomplete, data quality varies and providers' methods differ. The strongest reports combine analytics with customer due diligence,

transaction monitoring, behavioural indicators and open-source research. Where permitted by the applicable reporting framework, and where useful and proportionate, participants considered that relevant extracts or information explaining the analytics output may help the receiving FIU understand the basis of the assessment.

6. **Make analytics more transparent and pursue common standards**. Participants favoured developing standards on governance, taxonomy and explainability of blockchain analytics tools. This would improve comparability without stifling innovation.

7. **Join up the picture through cooperation**. Banks see fiat flows and customer profiles, CASPs see platform and on-chain activity, and authorities see across reports. Public-private and private-to-private dialogue, especially between banks and CASPs, helps close these gaps within legal limits. Public authorities have a role in building trust and facilitating that dialogue.

8. **Feedback improves reporting over time**. Case-by-case feedback is hard for stretched FIUs. Other channels can still help reporting entities learn what is useful and reduce defensive reporting, including typology and negative typology publications, thematic guidance, periodic quality feedback and structured dialogue.

A question mark remains around how far should reporting entities trace historical cryptoasset activity. Participants agreed that a proportionate approach is needed, but there was no common position on what that means in practice.

A typical case is a bank receiving funds from a MiCA-licensed CASP where the source of wealth is understood and there are no red flags. A licence is relevant but not decisive.

Related questions concern how much information institutions can reasonably request from customers, some of whom are reluctant to disclose wallet details for privacy and security reasons, and whether that reluctance should itself be treated as a risk indicator.

Developing that guidance – and continuing to work through the challenges and good practices indicated above to enhance their application in practice – is a joint task for public authorities and reporting entities. Initiatives and networks such as the Global Conference on Criminal Finances and Cryptoassets, the Wolfsberg Group and the Europol Financial Intelligence Public-Private Partnership (EFIPPP) are powerful forums to take that work forward.

Acknowledgements

The session was organised by Agnès Ciccarone (The Wolfsberg Group), Olga de Truchis (Société Générale), Greta Barkauskienė (Center of Excellence in Anti-Money Laundering) and Nico Di Gabriele (European Central Bank), acting in his personal capacity. The latter three moderated the two-hour event under the Chatham House Rule.

It took place during the 10th Global Conference on Criminal Finances and Cryptoassets, co-organised by the Basel Institute on Governance, Europol and UNODC, and hosted by Luxembourg's Bureau de gestion des avoirs (BGA) on 15 September 2026. The organisers thank the conference organisers and hosts, as well as all participants for joining and sharing their experience so openly.

Disclaimer

The report is an informal summary of workshop discussions. It does not represent or imply a common position of workshop participants and has not been adopted, endorsed or approved by the institutions with which individual organisers, moderators or participants are affiliated. Nothing in the report should be interpreted as defining the applicable legal threshold for suspicious transaction or activity reporting, or as legal, regulatory, supervisory or compliance guidance.

AI tools were used in preparing this publication in line with the Basel Institute's standards for responsible AI use.

Licence and sharing

You may share this publication under a Creative Commons BY-NC-ND 4.0 International licence.

Cover image: Designed by bearfotos – Magnific.com (adapted).

Suggested citation: Basel Institute on Governance and The Wolfsberg Group. 2026. 'Reporting suspicious crypto activity: Bridging supervisory expectations and operational realities.' Available at: baselgovernance.org/resources/publications/crypto-str-report.

We welcome feedback and contributions to this ongoing debate and invite you to contact us at info@baselgovernance.org or info@wolfsberg-group.org.

1 Introduction

The workshop was organised to examine the practical realities of crypto-related STR/SAR reporting and to facilitate dialogue between stakeholders involved in the identification, reporting, analysis and investigation of suspicious activity.

The discussions brought together perspectives from across the financial crime ecosystem, including reporting entities, supervisors, financial intelligence units and other subject-matter experts. The objective was to explore how regulatory requirements are applied in practice and to identify operational challenges that continue to affect reporting effectiveness.

The programme was structured around three broad themes:

1. Understanding what constitutes a useful and actionable crypto-related STR/SAR;
2. Examining key operational challenges and friction points encountered when preparing and assessing reports;
3. Exploring opportunities to strengthen cooperation and dialogue between public and private sector stakeholders.

Particular attention was given to issues that have become increasingly prominent in crypto-related investigations, including the use of blockchain analytics, attribution uncertainty, investigative expectations, data quality and information-sharing challenges.

The discussions also explored the growing interdependence between traditional financial institutions and cryptoasset service providers, highlighting both public-private partnerships and private-to-private cooperation as important mechanisms for improving reporting effectiveness.

Participants further examined the role that public authorities can play in facilitating dialogue, fostering trust and supporting information exchange across different parts of the financial system.

The report that follows seeks to reflect the principal themes that emerged during those discussions, highlighting both areas of convergence and issues on which differing views were expressed.

2 What constitutes a useful and actionable STR/SAR?

One of the most consistent themes throughout the workshop was the distinction between unusual activity and suspicious activity.

Participants from both the public and private sectors emphasised that the existence of an alert, red flag or adverse indicator should not automatically

result in the filing of a STR/SAR. Instead, reporting entities are expected to apply professional judgement, assess the available information and determine whether the identified activity gives rise to a genuine suspicion.

The discussions highlighted the importance of analytical quality. A useful report should do more than describe transactions or reproduce outputs generated by monitoring tools. It should explain why the reporting entity considers the activity suspicious, what investigative steps were undertaken, what information was reviewed and how the available evidence informed the final assessment. Particular emphasis was placed on the need to articulate clearly the rationale for suspicion rather than simply reporting unusual or unexplained activity.

Several participants observed that reports are often most valuable when they provide a coherent narrative that allows investigators and analysts to understand both the activity itself and the reasoning that led to the suspicion.

The quality of information was also identified as a critical factor, as explored in more detail in the next section. A complete report includes the information relevant to the concern, with enough context to support further analysis.

The following table summarises some of the key features of useful, actionable and high-quality reports:

More useful	Less useful
Based on a genuine suspicion, reached through professional judgement and assessment of the available information.	Filed automatically because an alert, red flag or adverse indicator was triggered.
Clearly explains *why* the reporting entity considers the activity suspicious.	Describes transactions or reproduces monitoring tool outputs without explaining the suspicion.
Sets out what investigative steps were taken, what information was reviewed and how the evidence informed the assessment.	Reports unusual or unexplained activity with no account of what was checked.
Tells a coherent story that allows analysts to understand both the activity and the reasoning behind the suspicion.	Presents disconnected facts that are hard to follow or interpret.
Focuses on information relevant to the concern, with enough context to support further analysis.	Includes everything available regardless of relevance, or too little context to act on.
Contains accurate identifiers and complete transaction data, ideally in a structured, machine-readable format.	Has missing or inaccurate identifiers, or data entered manually in inconsistent formats.

Combines blockchain analytics with other sources, such as customer due diligence, transaction monitoring, account activity and open-source research, and attaches the analytics output where available.	Treats a blockchain analytics result as the sole basis for suspicion.
Filed where, following an appropriate assessment, the applicable legal threshold for suspicion is met.	Filed solely because an alert was generated or solely because information remains incomplete, without an assessment of whether the applicable reporting threshold is met.
Updated as new information emerges and understanding of the activity develops.	Left unchanged even when later information changes the picture.

3 Effectiveness, quality and defensive reporting

The issue of defensive reporting emerged as one of the central themes of the workshop and was discussed from both public- and private-sector perspectives.

A recurring observation was the distinction between an alert, a concern and a suspicion. Several participants noted that reporting entities frequently encounter situations where activity appears unusual or triggers monitoring alerts, but where the available information does not clearly support a conclusion that the activity is suspicious. The discussion highlighted the practical challenge of determining when concerns should be escalated into a formal report and when additional investigation remains appropriate.

This challenge was often described as a tension between timeliness and completeness. Reporting entities may be criticised if information is reported too late, yet reporting too early may result in submissions that contain little more than an initial alert or preliminary concern. The issue was particularly acute in relation to smaller retail cases, where institutions may face difficult decisions regarding how much investigative effort is proportionate before reaching a reporting decision.

Several participants observed that uncertainty itself may sometimes drive reporting decisions. Institutions may choose to submit reports because they are unable to obtain complete information or because they wish to avoid criticism for failing to report a potentially suspicious case. From a public-sector perspective, however, it was repeatedly stressed that an alert or an unresolved question should not automatically be equated with suspicion. Reporting entities were encouraged to articulate clearly the reasoning underlying their assessment.

The discussion also explored whether increasing reporting volumes necessarily contribute to better outcomes. Participants from both sectors noted that

excessive volumes of low-value reporting may create operational challenges for reporting entities and authorities alike. Concerns were raised that a focus on quantity can divert attention from reports that contain genuinely actionable intelligence and may contribute to the perception that reporting has become a defensive exercise rather than an intelligence-led one.

Several speakers noted that organisations with more mature compliance frameworks and greater specialist expertise are often better positioned to distinguish genuine suspicions from routine alerts, resulting in more contextualised and actionable reporting. Effective reporting was widely seen as dependent on experienced analysts who understand both the relevant technologies and the broader financial crime context, rather than relying solely on automated alerts, risk scores or analytics outputs. Other participants further noted that reporting quality is influenced not only by the maturity of an institution's control framework, but also by the strength of its compliance culture.

At the same time, participants acknowledged that institutions operate within complex legal and supervisory environments and are often required to make decisions despite incomplete or evolving information. No common position emerged regarding the appropriate reporting threshold or the point at which uncertainty should result in an STR/SAR. However, there was broad agreement that reporting effectiveness should be assessed primarily through the quality, context and intelligence value of information provided to competent authorities rather than the volume of reports submitted.

Stronger feedback mechanisms were also identified as an important means of helping institutions better understand what information is most useful, improve investigative practices and reduce unnecessary defensive reporting over time.

4 Data quality and structured reporting

Data quality emerged as one of the most consistent themes throughout the workshop and was discussed extensively from both reporting entity and FIU perspectives.

Participants repeatedly stressed that the usefulness of an STR/SAR depends as much on the quality, completeness and structure of the information as on the underlying suspicion. Accurate identifiers, complete transactional information and a clear explanation of the basis for suspicion were consistently identified as critical enablers of effective analysis.

Particular attention was given to structured reporting. Participants emphasised that machine-readable formats are most effective when they capture comprehensive and consistent information on all relevant persons, entities, transactions and financial products involved in a case. This includes structured information on legal and natural persons, relevant transactions and associated

financial products, including bank accounts, payment accounts, virtual IBANs and cryptoasset accounts.

Several participants highlighted the benefits of XML-based reporting, whereby information is generated directly from an institution's internal systems and transmitted in a structured format rather than manually entered into reporting platforms. Beyond reducing manual errors and improving completeness, XML reporting was seen as facilitating automated processing and more efficient financial intelligence analysis. Participants noted that structured submissions can significantly enhance authorities' ability to identify relationships between reports and combine information that may initially appear unrelated.

The discussion also highlighted the growing importance of structured reporting in a cross-border environment. Information relating to the same customer, counterparty or activity may be reported by different institutions, in different jurisdictions and at different points in time. In some jurisdictions, XML reporting can also support the automated dissemination of relevant reports through cross-border FIU cooperation mechanisms, enabling information to be shared rapidly with other affected Member States. Participants observed that reports with limited intelligence value in isolation may become highly significant when combined with information held elsewhere, making reliable identifiers and structured data increasingly important for effective financial intelligence analysis.

Private sector participants also highlighted the practical challenges created by increasingly complex cryptoasset business models. In some cases, different functions may operate within the same corporate group but remain separated by internal information barriers. As a result, relevant information may emerge gradually across different parts of an organisation, requiring reporting entities to update earlier reports as their understanding of the activity evolves. Investigations can develop incrementally, with initially unrelated facts later revealing a broader pattern of potentially illicit conduct.

Overall, participants identified data quality, structured reporting, consistent identifiers and machine-readable reporting formats as essential components of more effective suspicious transaction or activity reporting, particularly as cross-border cooperation and analytical capabilities continue to evolve.

5 Blockchain analytics: Value, limitations and practical challenges

Participants widely recognised the value of blockchain analytics as an investigative capability. These tools can provide visibility into transaction flows, help identify links between entities, support network analysis and contribute to the detection of potentially illicit activity. For many institutions, they have

become an integral component of crypto-related investigations and an important source of information when assessing potentially suspicious activity.

At the same time, the discussion highlighted a number of limitations and areas requiring caution. One recurring concern related to attribution. Participants described situations in which activity initially appeared suspicious but was subsequently explained once additional information became available. In some cases, apparently unusual transaction patterns were ultimately linked to incomplete wallet attribution within an analytics tool rather than suspicious customer behaviour. Participants also noted that analytics providers may employ different methodologies, clustering techniques and data sources, which can occasionally result in different conclusions regarding the same activity.

The conversation therefore repeatedly returned to the importance of understanding both the capabilities and limitations of blockchain analytics, and of avoiding overly mechanistic reliance on analytical outputs. Participants stressed that blockchain analytics should generally be viewed as one component of a broader investigative process rather than as a standalone basis for suspicion. The most valuable reports were often considered to be those that combine blockchain analytics with other sources of information, including customer due diligence information, transaction monitoring results, internal account activity and open-source intelligence.

One example discussed involved a transaction initially flagged because of an indirect link to an address associated with terrorist financing concerns. The reporting entity subsequently supplemented the blockchain analysis with open-source research that identified additional indicators linked to extremist activity. The combination of blockchain analytics, internal information and external research significantly strengthened the intelligence value of the resulting report and illustrated the benefits of a layered investigative approach.

Behavioural analysis was highlighted as an important means of identifying potentially suspicious activity. Effective detection cannot be based exclusively on blockchain analytics looking solely at on-chain activity. Examples discussed included the identification of money-mule networks and coordinated activity through the analysis of transaction timing, clustering of bank accounts and customers, IP addresses, VPN usage and links to over-the-counter activity.

Participants also observed that authorities assessing a report may not necessarily have access to the same analytics platforms, datasets or attribution methodologies as the reporting entity. For this reason, some FIU representatives suggested that, where available, reporting entities should attach relevant blockchain analytics reports or extracts to their submissions. Providing the underlying analytical output can assist authorities in understanding the basis of the assessment and facilitate further analysis.

Many participants supported greater transparency regarding how blockchain analytics results are generated, including the underlying methodologies, attribution approaches and confidence levels. However, there was limited support for full standardisation of analytical models or datasets. Instead,

participants generally favoured the development of common standards for governance, taxonomy and explainability that would improve transparency, understanding and comparability of outputs of blockchain analytics tools while preserving methodological diversity and fostering continued innovation.

More broadly, participants observed that crypto-related STR/SAR investigations often involve different tools and investigative techniques from those encountered in traditional financial crime investigations. Nevertheless, a common principle emerged throughout the discussions: while advanced analytical tools can significantly enhance investigations, they cannot replace professional judgement, critical analysis and a sound understanding of how such tools operate, their inherent limitations and the significance of the outputs they generate.

6 The limits of evidencing and tracing historical cryptoasset activity

One of the most significant discussions concerned a question that extends well beyond blockchain tracing:

How far should reporting entities be expected to evidence and trace historical cryptoasset activity, and to what extent should residual uncertainty contribute to a suspicion assessment?

The discussion highlighted that this issue affects both traditional financial institutions and cryptoasset service providers.

Participants noted that investigations frequently require institutions to review historical activity spanning multiple years and involving numerous exchanges, intermediaries, self-hosted wallets and other blockchain transactions. In some cases, institutions may also seek to understand activity conducted through decentralised services or transactions involving counterparties that are no longer operational.

Several participants described situations in which the broad origin of wealth appears reasonably understood, customer explanations are generally consistent, and assets ultimately originate from a regulated service provider. Nevertheless, evidencing and tracing every stage of a customer's historical cryptoasset activity may be operationally difficult and, in some cases, impossible. This may be particularly challenging where activity spans multiple platforms, jurisdictions and technologies, or occurred at a time when record-keeping standards and regulatory frameworks were less developed.

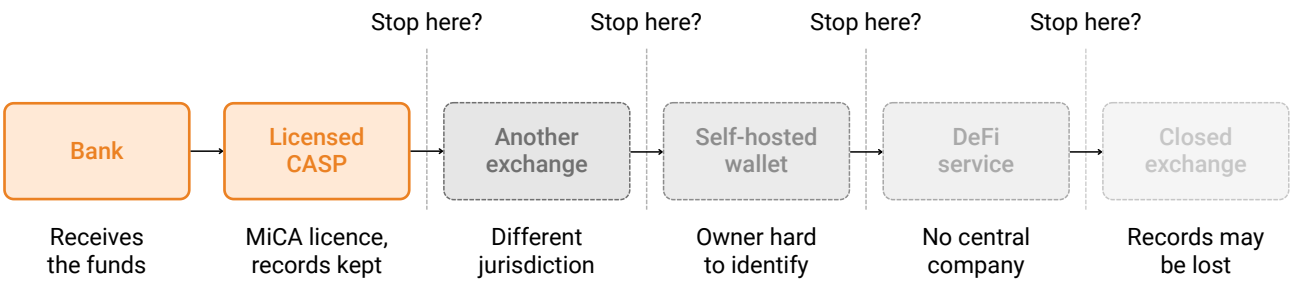


Figure 1. Illustrative example: how far back should a bank, for example, go to verify the source of funds? Possibilities and accuracy of tracing fade as one traces through multiple hops and platforms.

The discussion also touched on proportionality in information gathering. Several participants noted that some cryptoasset investors and entrepreneurs may be reluctant to disclose extensive wallet information, such as lists of wallet addresses, historical wallets and detailed holdings, because of privacy and personal security concerns. Questions were therefore raised regarding how far financial institutions should reasonably be expected to go in requesting such information and whether an unwillingness to provide it should, in itself, be regarded as a risk indicator.

These examples gave rise to broader questions regarding proportionality and evidentiary expectations. In particular, participants questioned how much evidencing and tracing of historical cryptoasset activity should reasonably be expected where a bank receives funds from a MiCA-licensed cryptoasset service provider, the broad source of wealth is understood, customer explanations are consistent and no obvious red flags have been identified.

While the involvement of a regulated provider was generally viewed as an important element of the risk assessment, several participants cautioned against assuming that all licensed providers present the same level of AML/CFT maturity, supervisory effectiveness or implementation standards. The existence of a licence was therefore viewed as a relevant factor, but not necessarily a decisive one when determining the extent of further enquiries required.

A recurring theme was the distinction between uncertainty arising from genuine risk indicators and uncertainty resulting from the practical challenges of evidencing and tracing historical cryptoasset activity. Some causes of uncertainty cut across both, as shown in the table below. While no common position emerged, many participants indicated that additional clarity regarding supervisory expectations, proportionality and the level of evidence reasonably expected in such cases would be valuable.

Uncertainty due to risk indicators	Uncertainty due to practical limits
Inconsistent customer explanations Links to high-risk addresses Unexplained transaction patterns	Old or missing records Platforms no longer operating
Activity across multiple jurisdictions Customers reluctant to share wallets	

7 Public-private and private-to-private cooperation

The discussions repeatedly returned to the importance of cooperation and information sharing as essential enablers of more effective suspicious transaction reporting.

Participants observed that crypto-related financial crime frequently spans multiple sectors of the financial system. Traditional financial institutions, cryptoasset service providers, payment firms and competent authorities may each observe different aspects of the same activity. As a result, no single institution is necessarily able to develop a complete understanding of a customer's activity or the wider context in which that activity occurs.

Against this backdrop, public-private partnerships were widely viewed as an important mechanism for improving effectiveness. Participants highlighted the value of regular dialogue between reporting entities, supervisors, FIUs and law enforcement authorities, particularly in a rapidly evolving environment where criminal typologies, technologies and business models continue to develop. Such engagement was seen as an important means of improving mutual understanding, identifying emerging risks and ensuring that reporting practices remain aligned with operational and national priorities.

Several speakers also emphasised the role supervisors can play in fostering constructive engagement with industry. Ongoing supervisory dialogue, thematic discussions and reviews of internal and external audit findings were seen as valuable tools for identifying weaknesses at an early stage and improving reporting quality. Close cooperation between supervisors and FIUs was viewed as particularly valuable in helping identify common weaknesses and communicate clear expectations to reporting entities.

Several participants drew parallels with established supervisory practices in other sectors such as banking supervision, noting that written guidance, supervisory findings and formal decisions are often most effective when complemented by direct dialogue. Meaningful exchanges between authorities and reporting entities can improve understanding of expectations, facilitate remediation of weaknesses and strengthen commitment to achieving better outcomes. Participants stressed that effective cooperation should operate as a genuine two-way dialogue, supported by mutual feedback and a shared focus on practical outcomes.

The workshop also devoted significant attention to private-to-private cooperation, particularly between traditional financial institutions and cryptoasset service providers. Several participants observed that the interface between traditional finance and the crypto ecosystem remains one of the areas where information asymmetries are most pronounced. Traditional financial institutions often have visibility over fiat transactions, customer profiles and broader account behaviour, while CASPs may have visibility over aspects of

the customer's crypto-related activity occurring within their platforms. As a result, each institution may hold information that is relevant to the other's risk assessment.

Many participants viewed stronger engagement between these sectors as an important opportunity to improve understanding of customer activity, reduce information gaps and support more informed decision-making. At the same time, participants acknowledged that legal, operational and confidentiality constraints may limit the extent to which information can be exchanged directly. This led to broader discussion regarding the role of public authorities in facilitating dialogue, fostering trust and enabling cooperation across different parts of the financial ecosystem.

Participants further noted that effective cooperation may need to extend beyond financial institutions and competent authorities alone. Examples were discussed of initiatives bringing a broader range of stakeholders from the digital asset ecosystem, such as technology providers and other unregulated firms. Such approaches were viewed as particularly valuable in breaking down silos, addressing information gaps and facilitating conversations that might not otherwise occur through traditional channels.

Feedback emerged as another recurring theme. Many reporting entities expressed a desire for greater insight into how submitted reports are used, what information is most valuable from an investigative perspective and which reporting practices contribute most effectively to financial intelligence outcomes. Participants noted that such feedback can help institutions refine investigative processes, improve report quality and better distinguish meaningful indicators from lower-value alerts.

One example highlighted involved a framework in which reporting entities assign an initial risk assessment to a report, while the FIU subsequently conducts its own analysis and provides periodic feedback on timeliness, completeness and overall reporting quality. Such mechanisms are valuable in helping reporting entities strengthen their investigative approaches and continuously improve the quality of reporting over time.

Authorities, however, highlighted the practical challenges associated with providing detailed case-specific feedback, particularly in environments characterised by increasing reporting volumes and limited resources. Nevertheless, there was broad agreement that stronger feedback mechanisms, whether through negative typology publications, thematic guidance, public-private dialogue or other channels, could play an important role in improving reporting effectiveness over time. FIUs were encouraged to take a proactive role in developing a common understanding of emerging threats, including through typology publications and ongoing engagement with reporting entities.

Overall, participants viewed public-private partnerships, stronger engagement between traditional financial institutions and cryptoasset service providers, and more effective feedback loops as important enablers of a more effective and intelligence-led AML/CFT framework.

Conclusion

The workshop highlighted the growing complexity of crypto-related STR/SAR reporting and the need to balance effectiveness, proportionality and sound judgement when assessing potentially suspicious activity.

More broadly, the discussions underscored the value of cooperation across the financial crime ecosystem. Better outcomes will require not only technological capabilities and high-quality information, but also stronger dialogue, information sharing and mutual understanding between public authorities, traditional financial institutions and cryptoasset service providers.

While no common position emerged on all issues, particularly in relation to the practical limits of evidencing and tracing cryptoasset activity, the discussions revealed broad convergence on a number of underlying principles, including proportionality, explainability, cooperation and intelligence-led approaches to financial crime risk management.

The discussions reinforced that the submission of an STR/SAR is not the end of the process. Rather, it marks the beginning of further financial intelligence analysis, investigative activity and, in some cases, measures aimed at protecting victims, disrupting criminal networks or preventing the dissipation of funds. The value of an STR/SAR should therefore be assessed not solely by its filing, but by its contribution to subsequent investigative and operational outcomes.

Ultimately, participants shared a common objective: improving the quality, usefulness and impact of STRs/SARs so that they provide meaningful intelligence and more effectively support efforts to detect, understand and disrupt illicit financial activity.

Key terms

Alert	An automatic warning from a monitoring system that a transaction or customer looks unusual. An alert alone does not mean the activity is suspicious.
AML/CFT	Anti-money laundering and countering the financing of terrorism. The laws, rules and controls designed to prevent these crimes.
Attribution	Linking a blockchain address or wallet to a real person, business or service.
Blockchain	A shared public record of all transactions on a cryptoasset network. Anyone can view it, but past entries cannot be changed.
Blockchain analytics	Software that follows the movement of cryptoassets on a blockchain to trace where they came from and where they went. Providers use different methods, so their results can differ.
Clustering	A technique used by blockchain analytics to group addresses that are likely controlled by the same person or service.
Competent authorities	Public bodies with the legal power to act on financial crime information, such as FIUs, supervisors and law enforcement agencies.
Cryptoasset service provider (CASP)	The EU term, under MiCA, for a business that provides cryptoasset services such as exchange or custody. It is similar to a virtual asset service provider (VASP).
Cryptoasset	A digital asset recorded on a blockchain, such as Bitcoin. Also called crypto, a virtual asset or a digital asset.
Customer due diligence (CDD)	The checks a firm must carry out to identify its customers and understand their activity and level of risk.
Decentralised services	Financial services run by software on a blockchain rather than by a central company. They are often called decentralised finance (DeFi). It can be hard to identify who is behind them.
Defensive reporting	Filing an STR mainly to avoid criticism or penalties, rather than because of a genuine suspicion. It produces large numbers of low-value reports.
Exchange	A company where people buy, sell and hold cryptoassets.
Explainability	How well the results of a tool, such as a risk score, can be understood and explained to others.
Fiat currency	Ordinary government money, such as euros or US dollars.
Identifier	Information that pins down a specific person, company or account, such as a name, date of birth, company number, IBAN or wallet address. Accurate identifiers allow authorities to link related reports.
Machine-readable (structured) reporting	Submitting reports in a fixed data format that computers can process automatically, rather than as free text.
MiCA	The EU's Markets in Crypto-Assets Regulation. It sets common EU rules for cryptoassets and for licensing and supervising CASPs.
Money mule	A person who lets their bank or cryptoasset account be used to move criminal money, knowingly or not.
Negative typology	A description of activity that may look suspicious but usually has a legitimate explanation. It helps firms avoid unnecessary reports.
On-chain	Activity recorded directly on a blockchain, as opposed to activity recorded only in a company's internal systems.
Over-the-counter (OTC) trading	Buying or selling cryptoassets directly between two parties or through a broker, rather than on a public exchange. It is often used for large trades.
Private-to-private cooperation	Information sharing between private companies, for example between a bank and a CASP, where the law allows it.

Proportionality	The principle that the effort and checks a firm applies should match the level of risk.
Public-private partnership (PPP)	Structured cooperation between public authorities and private companies to share information and expertise on financial crime.
Red flag	A warning sign that may point to financial crime, such as an unexplained large transfer. It needs further assessment before any conclusion is reached.
Regulated provider	An entity entitled (based either on registration or licence) to provide specified services and subject to the applicable regulatory and supervisory framework. Being subject to regulation is relevant to, but does not determine, the assessment of AML/CFT risk or the extent of due diligence required.
Reporting entity	A business that is legally required to report suspicious activity, such as a bank, CASP or payment firm.
Risk score	A number or rating produced by a monitoring or analytics tool to show how risky a transaction, address or customer appears.
Self-hosted wallet (unhosted wallet)	A wallet controlled directly by its user rather than by an exchange or other provider. It can be harder to identify who owns it.
Source of wealth	How a customer built up their overall wealth, for example through salary, business income, inheritance or investments.
STR/SAR	Suspicious transaction report or suspicious activity report. A report that a firm sends to the FIU when it suspects activity is linked to money laundering, terrorist financing or other crime.
Supervisor	A public authority that checks whether firms comply with AML/CFT rules and can take action if they do not.
Taxonomy	A common set of categories and labels, for example for types of risk in blockchain analytics, so that results mean the same thing across different tools.
Tracing	Following the movement of funds back to their origin or forward to their destination, across transactions, addresses and services.
Transaction monitoring	Systems that check customer transactions against rules or patterns and raise alerts when something looks unusual.
Typology	A description of a common method criminals use to launder money or finance terrorism. FIUs and others publish typologies to help firms spot these methods.
Virtual IBAN	An account number that routes payments into an underlying bank account, often used by payment firms. It can make it harder to see who is behind a payment.
VPN (virtual private network)	A service that hides a user's real IP address and location.
Wallet	A tool, either software or a device, that stores the keys needed to access and move cryptoassets.
Wallet address	A code of letters and numbers that shows where cryptoassets can be sent. It works like a bank account number.
XML	A standard data format that computers can read automatically. Many FIUs use it for structured STR submissions, for example through the goAML system developed by UNODC.

Basel Institute on Governance
Steinenring 60
4051 Basel, Switzerland

+41 61 205 55 11
info@baselgovernance.org
baselgovernance.org

The Basel Institute on Governance is an Associated Institute of the University of Basel.