Jersey Financial Services Commission

Thematic examination programme 2023

Feedback - virtual asset service providers' suspicious activity reporting systems and controls

Jersey Financial Services Commission

Glossary

AML/CFT/CPF	Anti-money laundering, countering the financing of terrorism and countering proliferation financing
Blockchain	Blockchain is a decentralised digital ledger that allows multiple participants to maintain a shared database without the need for a central authority.
Blockchain analytics	Blockchain analytics refers to the process of examining and interpreting data from blockchain networks to gain insights into transaction patterns and user behaviour. It involves leveraging various analytical tools and techniques to understand the flow of virtual assets within a decentralised ledger.
FATF	Financial Action Task Force
AML/CFT/CPF Handbook	Handbook for the prevention and detection of money laundering, the countering of terrorist financing, and the countering of proliferation financing
MLRO	Money Laundering Reporting Officer
ML/TF/PF	Money laundering, terrorist financing and proliferation financing
iSAR/eSAR	Internal Suspicious Activity Report / External Suspicious Activity Report
Supervised Person	As defined in Article 1 of the Proceeds of Crime (Supervisory Bodies) Law 2008. Includes persons regulated by the JFSC under one of the regulatory laws and registered persons including designated non-financial services businesses and professions (DNFBPs).
Supervisory Bodies Law	Proceeds of Crime (Supervisory Bodies) (Jersey) Law 2008
VASP	Virtual asset service provider
Virtual asset	A digital representation of value that can be digitally traded, or transferred and can be used for payment or investment purposes
VCEB	Virtual currency exchange business

Jersey Financial Services Commission

Contents

Jersey Financial Services Commission

1 Executive summary

During 2023, we assessed five virtual asset service providers' (VASPs) compliance with their statutory and regulatory obligations for suspicious activity reporting, including their relevant systems and controls. We also assessed the VASPs' transaction monitoring systems and controls.

The purpose of this feedback paper is to:

› explain our findings
› give examples of best practice
› inform VASPs of next steps

During the examination we found a number of issues related to:

› corporate governance
› completeness of suspicious activity reporting procedures
› employee training
› ongoing monitoring and scrutiny of transactions

VASPs and relevant supervised persons must now consider the findings and best practice highlighted in this feedback against their own arrangements.

2 Background

Before 30 January 2023, the only entities we regulated in the virtual asset sector were virtual currency exchange businesses, which have been in scope since 2016.

Following the Government of Jersey's alignment of Schedule 2 of the Proceeds of Crime (Jersey) Law with the Financial Action Task Force (FATF) definition of VASPs, virtual assets and their service providers were brought under our supervisory remit for the first time. This was our first examination of the newly defined VASP sector.

The interpretative note to FATF's Recommendation 15.7 sets out that in line with Recommendation 34, competent authorities and supervisors should establish guidelines and provide feedback to help VASPs apply national measures to combat money laundering, terrorist financing and proliferation financing (ML/TF/PF), and to detect and report suspicious transactions.

In the AML/CFT/CPF Handbook, VASPs' statutory and regulatory obligations for suspicious activity reporting are set out in Section 8.3.1 and 8.3.2, while systems and controls for the scrutiny of transactions and activity are set out in Section 6.

Our assessment of compliance with statutory and regulatory requirements was based on those in force during the review period.

3 Key areas for improvement

We identified four key areas for improvement.

1. **Corporate governance - board and senior management responsibilities - Section 2 of the Handbook.**

   Several findings related to board/senior management responsibilities and demonstrating effectiveness of systems and controls related to suspicious activity reports (SARs), including:

   › limited evidence that the board/senior management had given adequate consideration to potential trends, levels, or risks emerging from SARs

- minutes not sufficiently evidencing discussion relating to the money laundering reporting officer's (MLRO) function
- limited evidence to show the MLRO's reports had been discussed and/or challenged by the board/senior management

2. **Internal suspicious activity report (iSAR) and external suspicious activity report (eSAR) procedures – Sections 8.3.1 and 8.3.2 of the Handbook.**

   Several findings related to the completeness of iSAR and eSAR procedures, including:

   - not highlighting that reporting requirements extend to business relationships and one-off transactions that are declined
   - not including that SARs must be made regardless of the amount involved in a transaction or business relationship
   - not including the requirement for the MLRO to acknowledge any iSARs as soon as possible

3. **Training - Section 9 of the Handbook.**

   Several findings related to the adequacy of training procedures including:

   - training not tailored to the supervised person's business and ML/TF/PF risks
   - failure to cover relevant Jersey obligations
   - third party training solutions with inaccurate references to Jersey's AML/CFT/CPF regime

4. **Ongoing monitoring - Section 6 of the Handbook.**

   Several findings related to the adequacy of the systems and controls for ongoing monitoring and scrutiny of transactions, including:

   - transaction monitoring procedures that made no reference to the coverage and limitations of monitoring tools (Blockchain analytics or similar)
   - the frequency with which the system is updated

4 Findings and good practice

This section sets out our findings in more detail, along with examples of good practice (not all of which were identified during this examination).

We gave direct feedback to all examined supervised persons in the form of an examination findings report. Examined supervised persons were then required to submit a formal remediation plan, setting out the actions they will take and timescales for completion. We monitor these timescales.

Area of finding	Findings	Good practice
Board/senior management responsibilities	› board/senior management minutes did not sufficiently evidence discussion of the MLRO's performance and the MLRO's report	› demonstrated consideration of the effectiveness of systems and controls and of the quality of the management information being reported
	› insufficient consideration of the MLRO's timeliness in acknowledging iSARs	› the effectiveness of the MLRO and MLRO functions is assessed, including, but not limited to,

Area of finding	Findings	Good practice
	› insufficient evaluation of any competing priorities impacting the MLRO function › limited evidence of the board/senior management giving adequate consideration to potential trends, levels, or risks emerging from SAR reporting › minutes referred to a review of MLRO reports but did not evidence discussion and consideration of risks arising from an absence or increase in the level of SAR reporting in the period › limited evidence in minutes of actions considering the MLRO reports, such as a review of training or evaluating any deficiencies in analysing transaction monitoring reports › no record of ownership timeframes, dates for completion or conclusions for actions	whether the MLRO is dealing with SARs in a timely manner › routine assessment of whether the other roles the MLRO fulfils impact their effectiveness, independence, or give rise to conflicts › evidence in minutes of discussion/challenge/scrutiny and conclusions of the SAR information provided in MLRO reports › evidenced consideration of the levels/quality of SARs › resulting action points and owners documented and tracked to completion › reports not only "taken as read" or "noted" but evidence they are being discussed and considered in detail › evidence the board/senior management has undertaken separate training related to its own reporting obligations › evidence the MLRO/DMLRO have been/continue to be trained on handling iSARs/eSARs, liaising with the Joint Financial Crime Unit/law enforcement and how to deal with the risk of tipping off
iSAR/eSAR procedures	› not communicating to employees the identity of the MLRO (and any deputy MLROs) to whom an iSAR is made	› clearly stating that reporting requirements extend to potential business relationships and one-off transactions that are declined

Area of finding	Findings	Good practice
	› not highlighting that reporting requirements extend to business relationships and one-off transactions that are declined › not stating that SARs must be made regardless of the amount involved in a transaction or business relationship › not including the requirement for the MLRO to acknowledge any iSARs as soon as possible › not including the requirement to record all iSARs and eSARs in a register › not documenting that the MLRO is required to inform the Jersey Financial Intelligence Unit where relevant information is discovered › no established measures to prevent iSARs from being filtered by line management such that they do not reach the MLRO › not including the requirement to record all eSARs in a register with the date of the report and information to allow supporting evidence to be retrieved quickly	› maintaining registers to record all declined business, with a written explanation of the reason › the declined register (and analysis) forms part of the MLRO's board report › where relevant information is discovered, highlighting the requirement to inform the Jersey Financial Intelligence Unit and also evidencing this in MLRO reporting to the board › procedures and training include the requirement that the MLRO or (or Deputy MLRO) acknowledge iSARs as soon as possible › timescales for acknowledging iSARs form part of the MLRO board report and are analysed to ensure acknowledgements are made as soon as possible › iSARs are made in a set format › iSARs fully explain the information or matter which gave rise to knowledge, suspicion or reasonable grounds for knowledge or suspicion › iSARs include the date that the information or matter came to the employee's attention › iSARs include the date of submission of the iSAR › iSARS include full details of the customer, transaction or activity

Area of finding	Findings	Good practice
		that the supervised person holds on its records › tipping off provisions are covered in detail in procedures and written in a way that is easily understood for employees
Training	› materials not tailored to the activities and risks of the supervised person › failing to adequately cover relevant Jersey AML/CFT/CPF obligations including relevant mandatory sanctions legislation and obligations, and requirements about relevant connection to an enhanced risk state › adequate arrangements not in place to test the effectiveness of employee training and employee awareness › procedures incorrectly interpreting Article 4 of the Money Laundering (Jersey) Order 2008, and therefore incorrectly waiving due diligence for one-off transactions which do not exceed 15,000 euros › where third party training providers is used, instances of inaccurate references not reflecting Jersey's AML/CFT/CPF regime	› relevant to entity with specific examples of ML/TF/PF case studies, red flag warnings, examples of unusual activity, and customer profiling to identify unusual transactions › separately covering TF and PF as well as ML risks and prevention, with explanations of the differences between the three › including case studies to highlight the obligation of employees to report, the potential consequences of failing to report, and the importance each employee has in preventing and detecting financial crime › explaining risk appetite, business risk assessment and financial crime strategy and how these link to risk mitigation procedures › where a third-party training solution is used, assessing it to ensure it complies with the statutory and regulatory regime in Jersey, including a gap analysis to identify and address any deficiencies or inaccuracies › including financial sanctions in the training plan, with those who fail to achieve a minimum pass score in this area provided with additional training and reassessed

Area of finding	Findings	Good practice
		› analysing test answers to identify any areas with a lower level of understanding, which then informs future training › considering the guidance notes provided in Section 9 of the Handbook and referencing JFSC examination feedback papers
Transaction monitoring	› procedures not referencing monitoring to determine relevant connections to an enhanced risk state › no reference to the monitoring tool's (Blockchain analytics or similar) coverage, including how often the system is updated, or any limitations › policy not fully demonstrating compliance with the Money Laundering (Jersey) Order 2008 › policy not reflecting the Handbook's requirement of appropriate and consistent policies and procedures for the identification and scrutiny of transactions › lack of procedures for identifying complex or unusually large transactions, unusual patterns of transactions with no apparent economic or visible lawful purpose, and any other activity which may be related to the risk of ML/TF/PF	› detailed transaction monitoring procedures maintained which show the blockchain analytics solution used › documented evidence of understanding how the system works, including any limitations (and how these are managed) › systems tailored to the business › systems facilitate users applying additional judgement and experience in recognising unusual transactions and activity - particularly important when transactions are being made in virtual assets › procedures reference the monitoring undertaken to determine a relevant connection to an enhanced risk state and the associated training required for employees › and facilitates the application of additional judgement and experience to the recognition of unusual transactions and activity. This is particularly important when transactions are being made in VAs.

Area of finding	Findings	Good practice
	› insufficient evidence that transactions are scrutinised for notable or unusual activity › insufficient evidence of the measures in place to identify notable or unusual activity › insufficient evidence of the extent of examination and analysis of the monitoring outputs, exception reports and alerts	› transaction monitoring procedures reference the monitoring undertaken to determine a relevant connection to an enhanced risk state and the associated training required for employees. › evidence exists detailing how the transaction monitoring system works › assessments are undertaken when the system is changed › detailing the extent of the coverage/any limitations › detailing who or what is monitored, including details of the external data sources › detailing how the system is used to identify unusual activity › detailing how the outputs, exceptions reports and alerts are analysed

5 Additional Information on blockchain analytics

Blockchain technology enables transparency across virtual asset transactions through the immutable digital ledger that it provides. When a transaction is made, that data is forever stored on the blockchain. It cannot be amended and includes the data of every previous transaction made within that coin or token's history.

Blockchain analytics tools access and "scrape" this publicly available ledger and enable detailed oversight of the origins of funds, in addition to allowing users to see where the funds are sent. Consequently, such tools are fundamental in transaction monitoring and the identification of illicit activities involving virtual assets.

While supervised persons maintained transaction monitoring policies and procedures, we commonly found that these policies and procedures lacked sufficient detail on the blockchain analytics or screening tool used, alongside consideration of any limitations of the tool.

In addition to the examples of good practice set out in Section 3 above, we expect procedures to include:

- lists and data sources the supervised person uses for screening and monitoring transactions
- systems and controls demonstrating that the chosen transaction monitoring tool screens wallet addresses against all required sanctions lists and provides supporting documentary evidence
- the frequency with which the monitoring tool and the data it uses is updated - whether the solution updates in real-time or overnight
- simple, easy to follow procedure to help employees using blockchain analytics tools, including maps to support the visualisation of virtual assets

6 Action required

We have given direct feedback to all the VASPs we examined. The VASPs with findings were required to confirm remediation of such findings and/or submit a formal remediation plan setting out the actions to be taken and timescales for completion.

We expect boards and senior management of all VASPs, not just those subject to this examination, to now:

- consider the findings and best practice highlighted in this feedback against their own arrangements
- make changes to their systems and controls if they identify any areas for development
- ensure that their business is complying with all relevant statutory and regulatory requirements in relation to the completeness of their suspicious activity reporting systems and controls including, but not limited to Article 21 of the Money Laundering (Jersey) Order 2008 and Sections 8.3.1 and 8.3.2 of the Handbook
- consider the effectiveness of systems and controls and of the quality of the management information being reported, as set out in Section 2 of the Handbook
- demonstrate and evidence adequate scrutiny of transactions and activity under Section 6
- undertake appropriate training of employees under Section 9.5 of the Handbook

Supervised persons should also consider other relevant examination findings and questionnaires on the JFSC's website and related papers such as the role of the MLRO.

Where supervised persons identify any deficiencies in systems and controls, we expect them to:

- prepare a remediation plan and discuss this with their supervisor referring to our guidance on remediation action plans
- consider the notification requirements under the AML/CFT/CPF Code of Practice set out in Section 2.3 of the Handbook, and the relevant Code of Practice on dealing with the JFSC in an open and co-operative manner
- remedy any identified matters in the manner set out in the remediation plan agreed with their supervisor
- consider what assurance activities may provide comfort to the board and senior management that deficiencies identified have been addressed effectively

In future planning, we will consider repeating this thematic examination, to test whether VASPs have taken on-board the guidance set out in this feedback and whether the compliance rates have improved.