GIBRALTAR FINANCIAL SERVICES COMMISSION

DLT Provider Guidance Notes

Financial Crime

Introduction

The purpose of this guidance note is to provide a DLT Provider, as defined in the Financial Services (Distributed Ledger Technology Providers) Regulations 2020 (the DLT Regulations), with guidance as to the operational, technical and organisational standards expected and in some circumstances required by the GFSC.

This guidance note is specifically in respect of regulatory principle 8 of the DLT Regulations (the Regulatory Principle).

The Regulatory Principle states that "***A DLT Provider must have systems in place to prevent, detect and disclose financial crime risks such as money laundering and terrorist financing".***

This document should be read as interpretative guidance for a DLT Provider and the examples contained in this document should be noted as indicative of good practice by a DLT Provider in connection with the Regulatory Principle.

A DLT Provider should note that the GFSC will take this document into account when reviewing a DLT Provider's practices. The operational standards expected and required by the GFSC of a DLT Provider will vary depending on the size, particular nature, scale or complexity of the DLT Provider's business.

Scope and Applicability

A DLT Provider is defined as providing a Regulated Activity under the Financial Services Act 2019 and is therefore caught as a relevant financial business under the Proceeds of Crime Act (POCA).

The GFSC's Guidance Notes on 'Systems of control to prevent the financial system from being used for Money Laundering or Terrorist Financing activities' (AMLGNs) also apply to a DLT Provider. The AMLGNs should be read in conjunction with this Guidance Note. **The word "must" in section 33(2) of POCA imports an obligation on the Courts to "consider" the AMLGNs in determining whether a person has complied with POCA.**

The overarching requirements of the AMLGNs are six Statements of Principle that each firm must put in place in order to mitigate the risks that it is exposed to (please refer to chapter 4 of the AMLGNs for further details):

- SP1 The senior management of a firm is responsible for ensuring that the systems of control operated in the firm appropriately address the requirements of both the legislation and these guidance Notes.
- SP2 Firms must adopt a risk-based approach to these statements of principle and their requirements.
- SP3 All firms must know their customer to such an extent as is appropriate for the risk profile of that customer.
- SP4 Effective measures must be in place that require firms to have both internal and external reporting requirements whenever money laundering or terrorist financing is known or suspected.
- SP5 The firm will establish and maintain effective training regimes for all of its officers and employees.

- SP6 Firms must be able to provide documentary evidence of their compliance with the legislation and these Notes.

These additional notes provide sector specific guidance on mitigating measures and provides the risk context for this sector.

Risk and Context

The Financial Action Task Force (FATF) has recognised the need to adequately mitigate the money laundering and terrorist financing risks associated with virtual asset activities, and has set out detailed implementation requirements for effective regulation and supervision/monitoring of virtual asset services providers. For the purposes of complying with the FATF Recommendations, countries should consider virtual assets as "property," "proceeds," "funds", "funds or other assets," or other "corresponding value". By subjecting a DLT Provider to regulation and supervision and applying POCA to their activities, Gibraltar seeks to mitigate these risks.

Measures

In addition to the provisions of the AMLGNs, the following additional measures should be applied when a DLT Provider is establishing a business relationship or executing a one-off transaction. These additional mitigation measures are designed to be technology neutral.

It is therefore essential to the understanding of the AMLGNs, to determine whether the applicant business is undertaking a one-off transaction, or whether the transaction is the initial step in a business relationship as this can affect the verification requirements.

B2B versus B2C

A DLT Provider may be providing services and products to both Business-to-Business (B2B) and/or Business-to-Consumer (B2C) segments. Whilst the know your customer (KYC) requirements of POCA apply, it is important to differentiate on a risk-based approach, between the risks presented by both of these in the context of money laundering and terrorist financing risks. A DLT Provider must document its risk tolerance and assessment carefully for each of the products or services it offers in accordance with Chapter 6 of the AMLGNs.

Irrespective of the type of product or service provided, if there is a knowledge or suspicion of money laundering or terrorist financing, the obligation to submit a Suspicious Activity Report (SAR) under POCA applies.

B2B

In respect of B2B, it is very important for a DLT Provider to know the nature of its client's business, the managers and business owners, and the manner in which these operate.

A DLT Provider providing services or products on a B2B basis, which does not offer conversion of fiat currencies to any type of stored value and vice-versa, need not apply the transaction monitoring requirements of the AMLGNs to the B2B's underlying customers. However, the legal requirements contained in POCA shall continue to apply.

DLT Providers are not expected to have access to data relating to the customers of their B2B clients or request the same for money laundering or terrorist financing purposes. However, monitoring of B2B clients should include monitoring to ensure "*that the transactions are consistent with the relevant financial business's or person's knowledge of the customer, his business and risk profile, including where necessary the source of funds and keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date*", as set out in Section 12(2) of POCA.

Customer Due Diligence and Know Your Customer

The customer due diligence measures (CDD) and KYC requirements of POCA apply to a DLT Provider. However, the GFSC is keen to support new technologies and the emerging use of information and data to carry out due diligence (and not just reliance on documents) that enable easier management of CDD (see further below).

The GFSC will take a view on the adequacy of any new technologies used to support a DLT Provider to comply with its CDD and/or KYC obligations as part of the application process and in the context of a DLT Provider's business, product(s) and/or service(s).

A DLT Provider will be required to comply with CDD as set out in Part III of POCA.

A DLT Provider is also required to document the purpose and intended nature of a relationship and this must form part of the customer identification process. For further details, please refer to chapter 7.7.2.2. of the AMLGNs.

It is important to note that in this respect R91 of the AMLGNs states as follows:

The minimum due diligence requirements to satisfy customer identification documentation on nature and source of income or wealth is ascertained by documenting this to a level of "plausible verifiability".

The term "plausible verifiability" is made up of two constituents:

Plausible.

This is the documentation that the customer's economic activity is commensurate with the information that the firm will have before it through its due diligence processes. It should be clear to a firm when a customer is providing a source of economic activity that is incompatible with the information before it. In such cases the firm should consider the implications of such a statement or evidence and whether, as a result, a suspicious transaction report should be made to GFIU.

Verifiability.

This is documentation of the economic activity to a level of detail that would enable the firm, law enforcement agencies or other bodies to independently verify the source of income or wealth if the customer's risk profile increased, or money laundering or financing of terrorism was known or suspected.

It is clear from this that a description of "business man" would clearly be inappropriate as this is not verifiable. A description of "Management Consultant, MD of owner owned company X Management Consultants Limited of Number 1 The High Street, London, W23 1PX, UK" would be verifiable as the business and the address would be easily verifiable and the activity on the business relationship could easily be matched to the description provided. Again, any discrepancies between the information provided and the actual activity should prompt the firm to independently verify this information themselves or to make a suspicious transaction report.

A firm will be able to identify the country risk posed to it from the source of the income or wealth of the business relationship.

R92 As the business relationship's risk profile increases, the firm must move away from "plausible verifiability" to" independent verification" of economic activity in order to satisfy the customer identification documentation requirements in relation to the source of income or wealth.

R93 Independent verification requires that firms seek additional information on the economic activity of the business relationship from reliable and independent sources.

Simplified due diligence measures

The GFSC will consider representations made on a case-by-case basis, to allow DLT Providers to apply simplified due diligence in cases where they have:

- made a comprehensive risk assessment that determines that the transaction, product or service in question is deemed to be low risk; and
- they consider that they have sufficiently robust systems of controls.

Nonetheless, the traceability principles below need to be complied with in order to determine if one or more transactions are linked and result in this limit being breached. Similarly, if money laundering or terrorist financing is known or suspected, full KYC and SAR requirements apply.

Enhanced due diligence measures

A DLT Provider must apply enhanced due diligence measures in accordance with Chapter 6 of the AMLGNs. This includes in the following circumstances:

- for PEPs, family members of PEPs and close associates of PEPs;
- when dealing with a customer established in a high risk country; and
- where the firm has risk scored the customer as high risk.

eID for Verification of CDD Measures

The objective of CDD is to properly identify and verify parties (whether natural or legal persons) to a transaction or payment. Electronic identification and trust services (governed by the eIDAS Regulation - EU Regulation no 910/2014) are relevant when opening a business relationship with a DLT Provider.

Currently the eIDAS framework is one of the cornerstones of the Digital Single Market covering all elements of an electronic identification and authentication. A list of designated bodies, certified qualified signature creation devices, and certified qualified seal creation devices can be found here.

Where POCA refers to identifying and verifying a customer's identity on the basis of documents, data or information obtained from a reliable source, this should be read as also including electronic identification and relevant trust services as set out in Regulation 910/2014.

Traceability

A DLT Provider must know the identity of each and every customer and not process transactions where it does not know the customer's identity.

A DLT Provider must keep records of customer details and transactions including those on a distributed ledger so that holdings and transactions can be traced to each customer. These records must form part of the document retention processes of the DLT Provider and must be retained for a minimum of five years after the end of the business relationship or one-off transaction.

A DLT Provider should capture, record and retain unique identifiers of devices and network connections used by customers in communicating with the DLT Provider. Unique identifiers include (without limitation) IP address, MAC address, IMEI, ICCID, MEID, SEID and UUID. Recorded unique identifiers should form part of the document retention processes of the DLT Provider.

A DLT Provider should have systems to detect attempts by customers to circumvent CDD requirements or to obfuscate the nature and purpose of transactions. As part of its transaction monitoring processes, a DLT Provider should have systems to detect incongruity between information known about or provided by customers and information gathered during transactions. Incongruities and anomalies should be flagged, investigated and risk assessed for financial crime purposes.

Appointment and role of the Money Laundering Reporting Officer (MLRO)

DLT Providers are required to appoint an MLRO. Section 28 of POCA imposes a requirement on all relevant financial businesses to identify a person to carry out the function of the MLRO. Chapter 5 of the AMLGNs supplements the requirements by setting out that the overall responsibility for money laundering prevention lies with senior management and controllers of a firm. The MLRO is responsible for the oversight of the firm's anti-money laundering activities and is the key person in the implementation of the anti-money laundering strategy of the firm. The MLRO needs to be senior, free to act on his own authority and to be informed of any relevant knowledge or suspicion in the firm.

Outsourcing

A DLT Provider can choose to outsource some of its systems and controls and/or processing outside of its organisation and of Gibraltar. For example, some firms may outsource online ID verification, screening or the analysis of the provenance of virtual asset transactions to third party providers. Whilst third party resources may be used to assist the process, the firm is ultimately responsible for carrying out its own risk assessment of all potential customers. The outsourcing of a function does not exempt the DLT Provider

of its statutory and regulatory requirements. In all instances of outsourcing, it is the delegating firm that bears the ultimate responsibility for systems of control in relation to the activities outsourced. This will include the requirement to ensure that the provider of the outsourced services has in place satisfactory AML/CFT systems, controls and procedures, and that those policies and procedures are kept up to date to ensure compliance at all times, with the requirements of Gibraltar legislation, the AMLGNs and this guidance note.

Training

A DLT Provider must establish and maintain an effective training regime for all of its officers and employees, including senior management and Directors. A DLT Provider is expected to keep up to date with relevant tools and current technology to be able to analyse, detect and prevent the use of virtual assets for illicit activities and to ensure methods used are fit for purpose.

The obligations set out in Section 27 of POCA are expanded and clarified in the Chapter 9 of the AMLGNs.

Internal Audit

A DLT Provider must ensure that an independent audit is undertaken for the purposes of testing the below listed policies, controls and procedures in accordance with Chapter 5 of the AMLGNs:

- customer due diligence measures and ongoing monitoring;
- reporting;
- record keeping;
- internal controls;
- risk assessment and management; compliance management; and employee screening.

The frequency and extent of the audit shall be proportionate to the size and nature of the business.

GIBRALTAR FINANCIAL SERVICES COMMISSION

Published by:
Gibraltar Financial Services Commission
PO Box 940
Suite 3, Ground Floor
Atlantic Suites
Europort Avenue
Gibraltar

www.gfsc.gi