FijiFIU

Fiji Financial Intelligence Unit

Guideline 10

Financial Transactions Reporting Act

This Guideline is an enforceable instrument issued pursuant to the powers of the Financial Intelligence Unit under the Financial Transactions Reporting Act No.22 of 2004 [Section 25.1.j FTR Act & Regulation 35 and 37 FTR Regulations].

Use of Digital ID Systems/eKYC for Customer Due Diligence

1 INTRODUCTION

1.1 A financial institution[1] is required to identify its customers and verify that customer's identity.[2]

1.2 The customer identification and verification measures, also known as customer due diligence (CDD) measures, must be applied on a risk-based approach. This means that a financial institution may simplify or enhance its CDD processes and procedures depending on the risk of money laundering and terrorist financing of a customer, product, services and country or geographic location.

1.3 A financial institution must conduct CDD in the following circumstances:

(i) for all new customers, before or during the course of establishing a continuing business relationship with the customer;

(ii) for any occasional customer who conducts a transaction valued at $5,000 and above (including equivalent amounts in foreign currency);

(iii) for any existing customer for whom the financial institution has doubts about the adequacy of identification information previously obtained; and

(iv) for any customer whom the financial institution suspect is engaging in money laundering or terrorist financing activities.

1.4 Once a financial institution has established a continuing business relationship with a customer, it does not have to repeatedly identify and verify its customer's identity each time that customer conducts a transaction.

1.5 The objective of this Guideline is to provide further requirements and guidance to financial institutions on the use of digital ID systems for CDD purposes.

1.6 This Guideline is applicable to all financial institutions.

[1] Financial institutions include banks, non-bank financial institutions and non-financial businesses and professions that are covered by the FTR Act as specified in the Schedule of the FTR Act

[2] Section 4 Financial Transactions Reporting (FTR) Act (2004); Part 2 FTR Regulations; FIU Enforceable Guideline 4.

2 IDENTITY EVIDENCE TO VERIFY CUSTOMERS' IDENTITIES

2.1 A financial institution must identify its customer and verify that customer's identity *"on the basis of reliable and independent source documents, data or information or other evidence as is reasonably capable of verifying the identity of the customer."*[3]

2.2 The use of the terms "source documents, data or information or other evidence" means that a financial institution is not restricted in the form that the identity evidence may take in the customer verification process.

2.3 A financial institution therefore, may use *identity evidence* that consists of physical documentary evidence, digital records (such as scanned documents, photographs) or electronic record and information (such as databases, spreadsheets, software applications) to verify a customer's identity.

2.4 Furthermore, the identity evidence used by a financial institution to verify a customer's identity must be "reliable and independent", providing an appropriate level of confidence that the information provided by the customer (such as name, date of birth) are accurate.

3 DIGITAL ID SYSTEMS AND OTHER TECHNOLOGY BASED SOLUTIONS FOR CDD

3.1 **Electronic Know Your Customer** (eKYC) refers to a process of electronically verifying a customer's identity (whether a natural person or entity) using a digital ID system.

3.2 A "digital ID system" refers to the use of digital technology to capture, validate and store data on a person's identity. A person's identity information stored on a digital ID system is referred to as a "digital identity". A digital ID system can also be used to authenticate someone who claims a "digital identity".

3.3 A digital ID system may be provided by a government agency or on behalf of a government agency by a private sector entity.

3.4 Reliable and independent digital ID systems maybe used by financial institutions for CDD purposes when onboarding customers either on a face-to-face or non-face-to-face basis.

3.5 A digital ID system is considered reliable and independent when it provides a financial institution an appropriate or acceptable level of confidence (or assurance) that it will work as it is supposed to and will produce accurate results.

[3] Section 4(1) FTR Act

4 APPROVAL FOR USE OF DIGITAL ID SYSTEMS FOR CDD OR EKYC

4.1 A financial institution that intends to rely on a digital ID system provided by external parties for eKYC purposes must ensure that it:

a) understands the basic components of the digital ID system[4];

b) understands the level of confidence or assurance the digital ID system provides to determine its reliability and independence; and

c) based on the digital ID system's assurance level, decide whether the system is reliable and independent and can be used for eKYC purposes given the risk of money laundering and terrorist financing of a customer, product or geographic area of operation.

4.2 Government may authorise or endorse the use of a digital ID system(s) within a government agency or a private organisation for use by external parties such as financial institutions.

4.3 Where the government has not authorised a digital ID system for use for eKYC or has not provided a framework for determining a digital ID system's confidence/assurance level, a financial institution must assess and determine the reliability and independence of the ID system itself.

4.4 A financial institution must obtain Board and/or senior management approval on the overall risk management framework for the use of digital ID systems to conduct eKYC.[5]

4.5 A financial institution must develop and implement appropriate policies and procedures to address any risks arising from the use of eKYC. These include operational risk, IT risks and money laundering risks.

4.6 Where proper internal approval has been obtained to use eKYC for the first time, a financial institution must notify the Financial Intelligence Unit and/or Reserve Bank of Fiji (RBF) of its intention to implement an eKYC solution for CDD purposes.[6]

[4] Involves the identity proofing and enrolment component (such as how a person's identity information is collected, verified and established as an identity account on the system) and authentication component.

[5] Executive management approval must be sought for financial institutions or entities with no Board arrangement.

[6] All financial institutions licensed by the RBF such as insurance companies, banks and securities intermediaries must also notify the RBF. All other financial institutions that are not regulated by the RBF and all designated non-financial businesses and professions such as legal practitioners, accountants and real estate agents must only notify the FIU.

5 NON-FACE-TO FACE CUSTOMER DUE DILIGENCE

5.1 A financial institution may onboard customers on a non-face-to-face basis with minimum or no physical interaction. This means that the CDD process could be undertaken on a non-face-to-face basis.

5.2 Often a non-face-to-face CDD process involves eKYC.

5.3 When using non-face-to-face onboarding of customers, a financial institution must adopt additional procedures for verification of customers' identities, to complement the non-face-to-face due diligence process.[7]

5.4 These additional procedures are to verify that any digital identity evidence provided (e.g. electronic/scanned identification documents or reference numbers of identification documents) is reliable and that the customer's information provided within (e.g. name, date of birth) are accurate. These additional procedures may include:

a) verifying the applicant's/customer's information (such as name, date of birth) against a reliable and independent digital ID system or public registries; or

b) checks to verify the security markers/features in "soft copies" of identification documents to determine its authenticity.

5.5 Furthermore, a financial institution must adopt additional procedures to establish that the person claiming a "digital identity" (customer to be on boarded) and presenting the digital identity evidence (credentials) is the rightful owner of that identity. This additional procedure is known as an "authentication process" and must rely on one or more factors relating to:

a) something a person has (such as a card, security token, mobile app);

b) something a person knows (such as a password, PIN, passphrase); or

c) something a person is (such as a person's fingerprint, irises, face, voice).

5.6 The use of video-conferencing (where the financial institution engages with the customer and sights his/her identification documents over a video call) is not sufficient when used on its own. If a financial institution employs video conferencing to onboard a new customer, this must be supplemented by additional verification procedures (refer to paragraph 5.4).

5.7 Furthermore, a financial institution may also delay the verification of the customer on boarded through non-face-to-face basis.[8]

5.8 These *additional procedures* are aimed at mitigating the higher risk of fraud (fake identity) and impersonation associated with the use of digital identity evidence presented/submitted by customers during the non-face-to-face onboarding process.

[7] Regulation 11 FTR Regulations
[8] Regulation 15 FTR Regulations

6 ONGOING CONTROL MEASURES WHEN IMPLEMENTING EKYC

6.1 A financial institution must continuously monitor its eKYC processes and solutions to ensure that it is effective and accurate.

6.2 When using eKYC processes, a financial institution must ensure that proper records of the customer's identity and the evidences used to verify the identity of the customer are maintained.

6.3 A financial institution must have access to or have a process for enabling regulatory authorities including law enforcement agencies to obtain identity information and evidence for its customers.

7 OVERSIGHT AND IMPLEMENTATION

7.1 The FIU and/or the relevant supervisory authority, in the course of its supervision, may assess the compliance of all financial institutions with the requirements of this Guideline.

7.2 Non-compliance may result in sanctions as specified in section 43(2) of the FTR Act and regulation 42(2) and 42(3) of the FTR Regulations.

7.3 This Guideline is effective from 31 January 2024.

Financial Intelligence Unit

6 October 2023