GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT
OF TRINIDAD AND TOBAGO
MINISTRY OF FINANCE

FIUTT REFERENCE: ADV/003/2025

ADVISORY TO REPORTING ENTITIES: ONBOARDING FRAUD

The Financial Intelligence Unit of Trinidad and Tobago ("the FIUTT") is publishing this Advisory in accordance with *Section 17(1)(b) of the Financial Intelligence Unit of Trinidad and Tobago Act, Chap. 72:01, and Regulation 26(1)(d)(ii) of the Financial Intelligence Unit of Trinidad and Tobago Regulations.*

PURPOSE OF THIS ADVISORY

This *Advisory* is intended to:

Notify Financial Institutions (FI's), Non-Regulated Financial Institutions (NRFI's) and Listed Businesses (LB's) about the growing risk of "**Onboarding Fraud."** In Onboarding Fraud, fraudsters exploit the account creation process by submitting stolen, fabricated or altered documents to establish accounts, obtain unauthorised access to services and commit financial crimes. The FIUTT hopes that this Advisory will assist FI's, NRFI's and LB's in identifying within their own organisation, the specific vulnerabilities illustrated and provide guidance on best practice measures aimed at mitigating such risks.

GENERAL INFORMATION

The FIUTT has observed a notable increase in Suspicious Transaction/Activity Reports wherein malicious actors are exploiting weaknesses in the customer onboarding process by presenting themselves as legitimate clients. These individuals often submit stolen, fabricated, or altered identification and supporting documents to establish or reactivate financial accounts. This is manifested in the following inferred actions:

- **Fraudulent or altered KYC Documents:**
  - Submission of utility bills with unassigned or invalid meter numbers.
  - Submission of utility bills issued in the names of unrelated third parties.
  - Submitted fraudulent utility bills are frequently tied to recurring addresses identified as a nexus for multiple suspected fraudsters.
  - Submission of employment verification letters from non-existent or unverifiable employers.
  - Submission of employment verification letters that have noticeable font or formatting inconsistencies.
  - Reuse of documents by the same individual for multiple accounts, suggesting deliberate fabrication to support financial activity
  - Submission of fabricated or "photo-shopped" documents and images during digital onboarding, enabling the creation of accounts with stolen identities.

- **Shared or Unauthorized Residential Addresses**
  - Provision of addresses already associated with other clients, sometimes accompanied by authorization letters allowing unrelated persons to claim residence.
  - Repeated use of the same address across multiple onboarding attempts, indicating attempts to bypass verification controls.

- **Suspicious Employment and Network Links**
  - Employment histories tied to previously flagged entities or companies implicated in prior suspicious transactions.
  - Connections to other individuals through shared documentation, addresses or transactional activity, suggesting potential collusion or systematic misuse of KYC materials.
  - Networked activity among multiple accounts, identifies and addresses indicates organized onboarding fraud schemes, where individuals coordinate to exploit verification weakness systematically.

This Advisory highlights the exploitation of customer on-boarding processes within financial institutions by individuals who submit falsified, stolen, or manipulated documentation to gain unauthorized access to financial services. It also addresses the need for robust controls and safeguards to mitigate the risks associated with onboarding fraud, including the creation of accounts using false identities, synthetic identifies, or documents linked to other suspicious clients.

Source: https://www.hitrust.com/blog_Fraudsters.html

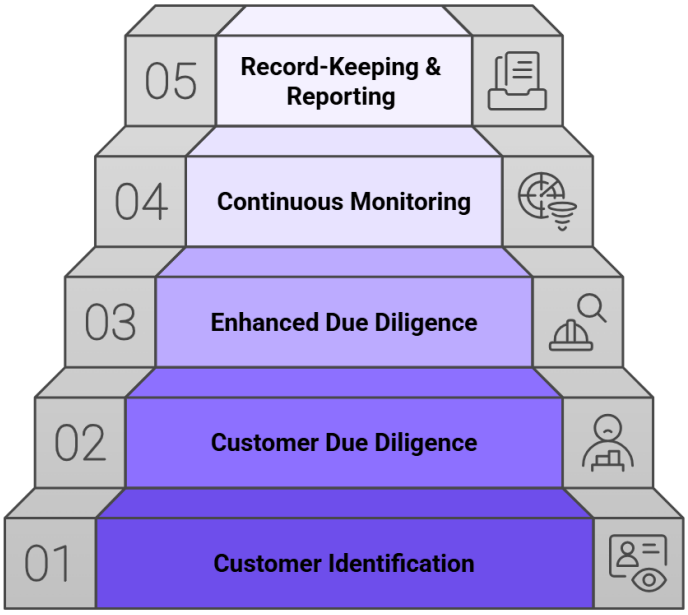
Pursuant to the Financial Obligation Regulations (2010) Regulation 11 (1), every FI and LB, are required to implement robust customer due diligence and risk mitigation measures to prevent on-boarding fraud and related illicit activities.

Regulation 15 mandates that FIs and LBs, upon initiating a business relationship or transaction, must obtain and verify relevant identification records of the applicant. These records must include full name, permanent address with proof, date and place of birth, nationality, nature and place of business or occupation where applicable, occupational income where applicable, signature, purpose of the proposed business relationship or transaction and source of funds, as well as any additional information deemed appropriate by the institution. A valid passport, national identification card, or driver's permit must be obtained or examined as proof of identity.

On-boarding fraud poses significant financial, reputational and regulatory risks to businesses and consumers. It can lead to financial losses through uncollectible debts, chargebacks and unauthorized transactions. Critically, on-boarding fraud also elevates the risk of money laundering and other illicit financial activity, exposing institutions to severe regulatory and compliance consequences.

The on-boarding process represents the critical first point of contact between the institution and its' customers, making it the most effective stage to prevent fraud. By implementing robust **Know You Customer (KYC)** procedures during on-boarding, such as identity verification, document authentication and risk assessment, institutions can confirm the legitimacy of their customers, reducing exposure to financial and reputational risks. Strengthening controls at this stage not only protects the institution from fraud but also establishes a secure and positive customer experience grounded in trust and compliance.

The 5 Steps in the KYC Process



Source: https://www.fraud.com/post/kyc-process

RECOMMENDATIONS FOR CONSIDERATION BY REPORTING ENTITIES (FI's, NRFI's and LB's)

The FIUTT proposes that FI's, NRFI's and LB's protect themselves from on-boarding fraud and safeguard the integrity of the financial sector by implementing enhanced preventative measures, including more stringent **Know Your Customer (KYC)** protocols such as**:**

- **Implement Robust Identity Verification Processes:**
  - Verify information against trusted databases and cross-check employment, residential and financial details.
  - For foreign customers, obtain references from their financial institutions.

- **Leverage Advanced Technologies** *(where applicable)***:**
  - Use machine learning to analyse large datasets for anomalies and patterns indicative of fraud.
  - Employ document verification tools to detect fake or altered IDs, photo-shopped images and synthetic identities.

- **Conduct Risk Assessment and Enhanced Due Diligence**:
  - Evaluate the risk profile of each customer based on factors such as geography, transaction patterns, occupation and connections to high-risk entities.
  - Apply enhanced due diligence for high-risk clients or accounts with large transactions, including verifying the source of funds and conducting background checks.
  - Enhanced Due Diligence Measures
    - Verify utility bills, employment letters and other supporting documents directly with issuing entities.
    - Require multiple proofs of address where suspicion arises.
    - Conduct deeper background checks for high-risk clients or unusual account activity.

- **Rigorous Document Scrutiny:**
  - Use a checklist to spot anomalies such as font inconsistences, unassigned meter numbers or addresses that appear repeatedly.
  - Utilise digital verification tools to authenticate submitted documents.
  - Wherever possible, verify utility bills and employment letters directly with the issuing companies.

- **Address Verification:**
  - Cross-check addresses against existing customer records to identify unusual overlaps.
  - Flag repeated use of the same address across multiple accounts as a potential red flag.
  - Require additional proof of residence when customers provide shared or previously flagged addresses.
  - In suspicious cases, independently verify residential addresses provided by clients, including physical visits or third-party address verification services.

- **Ongoing Transaction Monitoring**:
  - Implement real-time systems to identify activity inconsistent with customer profiles, including unusual cash deposits, rapid fund transfers, high-volume withdrawals or layering techniques.
  - Continuously monitor accounts for connections to previously flagged addresses, clients or suspicious transactions.

This space was intentionally left blank

- **Employee and Customer Education:**
  - Conduct regular training for frontline staff to recognize/detect inconsistencies in documents, such as fonts, signatures, dates or formatting anomalies as well as unusual on-boarding behaviour.
  - Foster a culture of vigilance where suspicious cases are promptly escalated.

- **Establish Clear Policies and Procedures:**
  - Develop and enforce detailed on-boarding and verification guidelines.
  - Regularly review and update these procedures to reflect evolving fraud tactics and regulatory changes.

- **Inter-Institutional Cooperation** *(where permissible)***:**
  - Share relevant information, patterns and red flags with the FIUTT and other financial institutions to detect and prevent fraud networks.

- **Group/Interdepartmental Collaboration:**
  - Strengthen communication between branches, compliance and fraud investigation units to flag and share emerging fraud trends quickly.
  - Maintain a centralized, regularly updated watch-lists of high-risk addresses, individuals or companies known to be involved in fraudulent activities.

Financial Institutions, Non-Regulated Financial Institutions and Listed Businesses are reminded that any transaction/activity suspected to be fraudulent or related to money laundering, financing of terrorism or any other predicate offence, should be reported:

- by the immediate submission of STRs/SARs, to the FIUTT, and;
- immediately to the Fraud Squad of the Trinidad and Tobago Police Service (TTPS) at Telephone numbers: 1(868) 625-2310 or 1(868) 623-2644 or; Fraud Squad South office at 1(868) 652-8594; or by Email: Fraud.Squad@ttps.gov.tt

Dated: October 06, 2025
Financial Intelligence Unit of Trinidad and Tobago