GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT OF TRINIDAD AND TOBAGO
MINISTRY OF FINANCE

FIUTT REFERENCE: ADV/001/2025

ADVISORY TO FINANCIAL INSTITUTIONS: KNOW YOUR EMPLOYEE (KYE)

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:

Apprise Financial Institutions (FI's), Non-Regulated Institutions (NRFI's) and Listed Businesses (LB's) with information on the apparent vulnerabilities of FI's, NRFI's and LB's regarding the likely involvement of **"compromised employees"** in facilitating **"Nominee or Straw Borrower Loans."** The FIUTT hopes that this Advisory will assist FI's, NRFI's and LB's in identifying within their own organization, the specific vulnerabilities illustrated and provide guidance on best practice measures aimed at mitigating such risks.

GENERAL INFORMATION

The FIUTT has noted increased Suspicious Transaction/Activity Reports wherein the employees of some Financial Institutions 'appear to be colluding with external parties to facilitate **Nominee or Straw Borrower Loans,** in which the borrower named in the loan documents is not the real party of interest i.e. the party that receives the use or benefit of the loan proceeds. This is manifested in the following alleged/inferred actions:

- Employees of FI's **performing multiple roles in the loan process** such as approving and disbursing loans, thereby bypassing critical internal controls.
- Employees of FI's **approving loan applications with falsified or incomplete documentation** despite clear red flags such as recurring use of identical templates and inconsistent information.
- Employees of FI's **approving loan applications in which multiple borrowers listed the same referrals**, who in some cases were presented with variations in name spelling and different phone numbers.
- Employees of FI's **making no attempt to directly validate supporting documents** with the issuing agencies.
- Employees of FI's **approving renewals for loans with persistent past-due histories** without adequately investigating the cause of non-repayment.
- Employees of FI's **inaccurately reporting loans with persistent past-due histories as current**, effectively concealing them from the institution's problem loan portfolio.
- Employees of FI's **failing to uphold due diligence standards,** such as conducting site visits, crucial for confirming the legitimacy of projects for which loans are being sought, or conducting site visits superficially.
- Employees of FI's **failing to detect and flag irregularities** in the application process such as a dormant account containing a minimum sum suddenly receiving a large, unexplained cash deposit prior to securing the loan.
- Employees of FI's **coaching loan applicants** on how to respond during interviews.
- Employees **connecting loan applicants with third-parties** willing to provide the required cash down payments as security.
- Employees of FI's **approving excessive loan applications for borrowers with familial ties**, shared mailing addresses or overlapping work histories, disregarding clear relationships and allowing interconnected loan applications to proceed without proper scrutiny.
- Employees of FI's **approving loan applications in cases where borrowers were observed making payments into each other's accounts.**

This Advisory highlights the manipulation of the internal processes/systems within financial institutions by 'compromised' employees who wittingly, and/or, unwittingly facilitate money laundering, or are themselves engaged in criminal activity. It also addresses the need to mitigate the risks associated with potentially 'compromised' employees.

Pursuant to the Financial Obligation Regulations (2010), Regulation 5(1) directs that every FI, NRFI, and LB, shall utilise best practices of the industry, to determine its staff recruitment policy, with the use of which, **staff of the highest levels of integrity and competence, shall be hired and retained.**

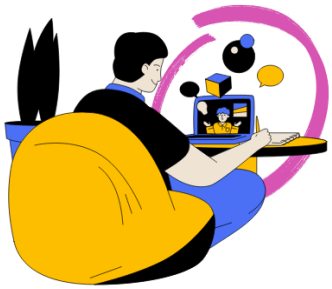
In addition to a robust recruitment policy, FIs, NRFIs and LBs should **implement ongoing monitoring of employees** to ensure that they continue to meet the institution's standards of integrity and competence.

Know Your Employee (KYE) processes assists in mitigating the risk of insider threats as it limits employee fraud, guards against money laundering, manages employee on-boarding and access control, builds and retain consumers trust as well as improves employee loyalty.

BENEFITS OF KNOW YOUR EMPLOYEE (KYE)

Know *Your* Employee

Know Your Employee (KYE) is the process of verifying the identities and backgrounds of current and potential staff.
It aims to ensure employees are legitimate and do not pose a risk due to past criminal activity.



KNOW YOUR EMPLOYEE

Limiting Employee Fraud	Guarding Against Money Laundering	Managing Employee Onboarding
• Employees with access to sensitive systems and resources may exploit their privileges to misappropriate assets, funds, or business opportunities. Implementing Know Your Employee (KYE) protocols allows organizations to identify individuals with questionable histories, enabling proactive oversight or exclusion to safeguard against internal threats.	• To combat money laundering, it is vital for financial institutions to implement Know Your Employee (KYE) measures. Criminal networks may target employees to exploit procedural gaps and facilitate the movement of illicit funds. Through KYE, institutions can screen out high-risk candidates and monitor existing staff for potential associations with money launderers, thereby strengthening internal defenses against financial crime.	Effective employee onboarding and access control are crucial in preventing impersonation and credential fraud. Know Your Employee (KYE) ensures that both current and prospective employees are properly verified, confirming their identities and assigning access permissions that align with their roles, thus mitigating the risk of unauthorized activity.

RECOMMENDATIONS FOR CONSIDERATION BY FI's, NRFI's and LB's

The FIUTT proposes that FI's, NRFI's and LB's protect themselves by implementing mitigating measures and safeguard the integrity of the financial sector through the implementation of more stringent **Know Your Employee (KYE) measures including:**

- **Thorough Pre-Employment Screening:** Hiring trustworthy employees is a key fraud prevention strategy. Pre-employment screening is the first line of defence against fraud. To reduce exposure and avoid fraudulent activity, FI's, NRFI's and LB's should have clearly defined pre-employment standards. These standards should include:
  - ***All candidates should be required to complete a detailed application form:*** They must be informed that the organisation conducts thorough background checks and may be asked to sign a release form or equivalent document authorising the process.
  - ***Referee and Employment Verification***: References and former employers (e.g. directors and or supervisors), should be contacted after verifying their identities independently.

- ***Verification of Qualifications***: All educational certificates should be thoroughly examined and independently verified.
- ***Comprehensive Background Checks****:* Background checks should be conducted using publicly available databases and information sources to identify any potential conflict of interests, bankruptcy records, media and social media mentions. Criminal record checks should also be considered to assess any prior legal issues as well as credit checks.

- **Develop a Comprehensive Fraud Control Policy Document**: Implementing a clear and comprehensive fraud control policy is crucial for effective prevention. Employees can only follow procedures if they are clearly outlined and documented. FI's, NRFI's and LB's should ensure that all procedures are documented, accessible, and accompanied by training. Regular reports on their implementation should be submitted to senior management, and a strict "zero tolerance" stance on breaches and adherence to the procedures should be maintained.

- **Establish a Robust Code of Ethics**: FI's, NRFI's and LB's should establish a code of conduct that not only outlines the organisations expectations for ethical behaviour but also explicitly states that any form of fraud, regardless of its level, will not be tolerated and will be reported to the authorities. Additionally, the code should clearly define what constitutes employee fraud, an area that often cause confusion. By providing these clear guidelines, employees will understand the seriousness of fraudulent activity and the consequences for engaging in such actions.

- **Policy Awareness and Staff Education:** To minimise the opportunity for employees to commit fraud, FI's, NRFI's and LB's should train staff on company policies and procedures during the hiring process and periodically for reinforcement. A clear code of conduct outlining expectations and consequences should also be implemented. FI's, NRFI's and LB's should also require employees to review and acknowledge this code annually. The Management /Leadership of FI's, NRFI's and LB's must also lead by example by consistently following established protocols.

- **Strengthening Internal Controls Through Role Separation:** No single employee should be responsible for an entire transaction process from beginning to end. FI's, NRFI's and LB's should ensure that there is proper segregation of duties by distributing responsibilities among staff so that no single employee controls multiple critical functions. For example, loan approval and disbursement should always be handled by separate individuals, regardless of seniority.

- **Monitoring Employee Behaviour for Fraud Indicators:** Certain employee behaviour can signal a higher risk of fraudulent activity, such as, consistently working outside of regular business hours or avoiding taking leave. This practise may suggest an attempt to work unsupervised. Other red flags or conditions that are abnormal in nature or differ from the norm include living beyond their means, neglecting to complete necessary reports and reconciliations, or consistently submitting compliance documents late. These behaviours while not definitive, should be closely monitored as they may point to potential misconduct.

- **Establish Periodic Oversight Mechanisms**: FI's, NRFI's and LB's should engage independent professionals to periodically review financial records as both a deterrent to potential fraud and as a means of early detection. These impartial assessments will provide a critical layer of oversight,

helping to identify irregularities before they escalate, thereby safeguarding the organisation from significant harm.

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: April 16, 2025

Director
Financial Intelligence Unit of Trinidad and Tobago