GOVERNMENT OF THE REPUBLIC OF TRINIDAD AND TOBAGO

FINANCIAL INTELLIGENCE UNIT
OF TRINIDAD AND TOBAGO
MINISTRY OF FINANCE

ADVISORY TO FINANCIAL INSTITUTIONS AND NON-REGULATED FINANCIAL INSTITUTIONS: KITING SCHEMES

FIUTT REFERENCE: ADV/007/2024
Issued : August 21, 2024

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

The purpose of this *Advisory* is to assist Financial Institutions (FIs) and Non-Regulated Financial Institutions (NRFIs) in identifying suspicious transactions relative to ***Kiting Schemes***.

It is intended to assist Compliance Officers in understanding the mechanics of kiting schemes and recognising the key characteristics in order to effectively mitigate the risks associated with this fraudulent activity. It is expected that Compliance Officers will share **the information contained in this Advisory** (not the Advisory itself), to the relevant staff.

The FIUTT hopes that this Advisory will assist FIs and NRFIs in identifying individuals that may pose a risk and provide guidance on best practice measures aimed at mitigating such risks.

GENERAL INFORMATION

The FIUTT has noted increased Suspicious Transaction/Activity Reports (STRs/SARs) wherein individual customers are benefitting from a delay in the bank's financial management system. Prior to the fraud occurring, the accounts were funded by either cash or Inter Bank (IB) credits. In most instances, these credits were followed by immediate ABM withdrawals for the entire amount. Consequently, the accounts were left in an overdrawn state. This pattern appears to resemble a ***kiting scheme***, where the value of the account balances is artificially inflated, giving unauthorised access to funds.

BACKGROUND

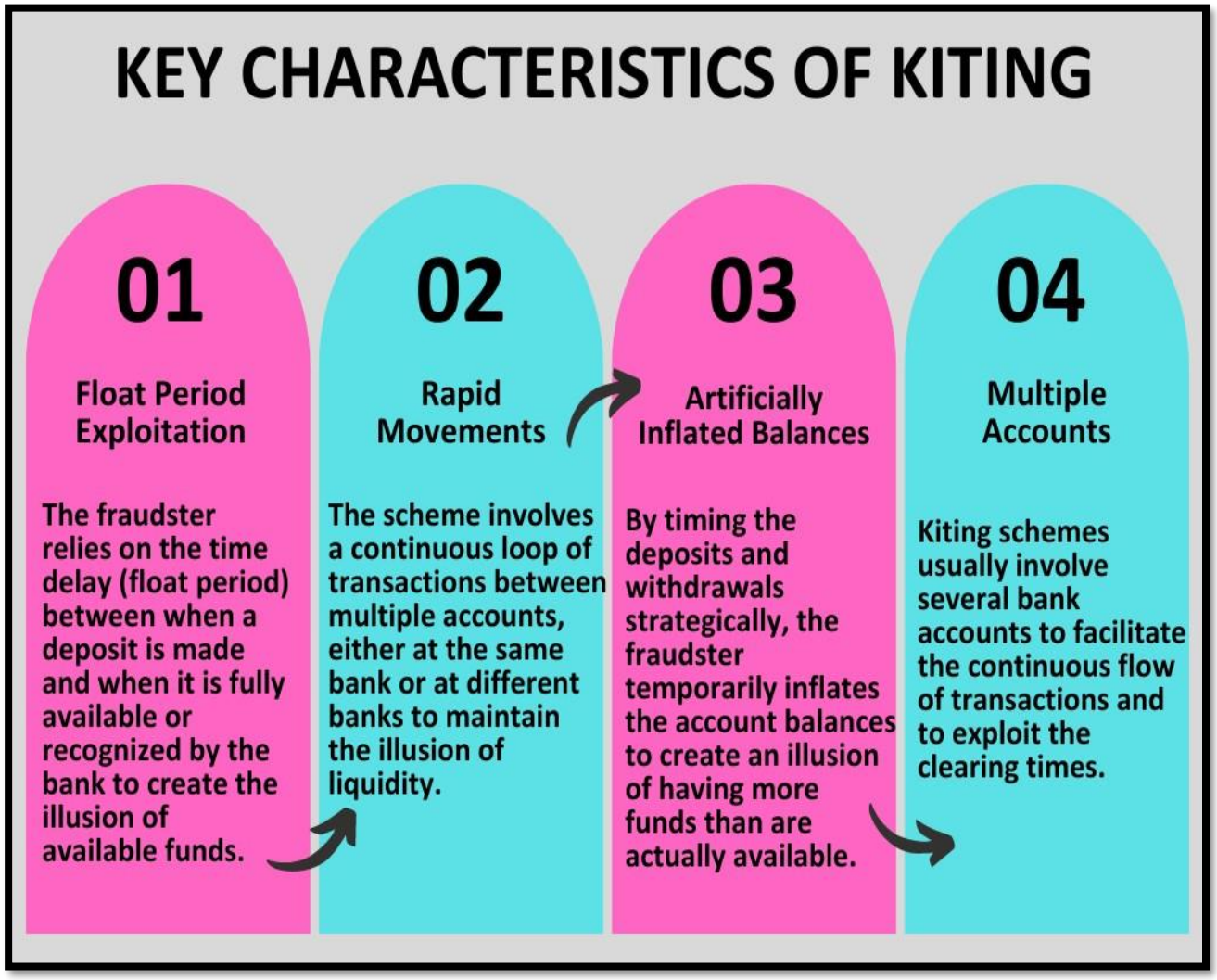
Kiting is a sophisticated form of financial fraud that exploits the lag time or float period between transactions to two or more bank accounts to artificially inflate account balances and create unauthorised credit. The most common forms of kiting include, cheque kiting, cash kiting and credit card kiting.

1. **Cheque Kiting:**
   This occurs when a person writes a check from one bank account, knowing there are insufficient funds, and deposits it into another account. Before the check clears, they write another check from the second account back to the first to cover the first check, thus creating a cycle of fraudulent balances. This exploits the time it takes for checks to clear between banks, allowing the perpetrator to have access to non-existent funds.

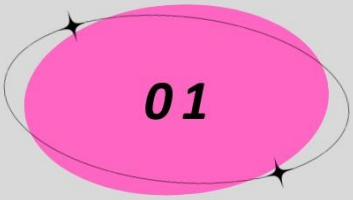
2. **Cash Kiting:**
   This scheme exploits the use of overdraft facilities and the lag time or float period before the funds are fully available or recognised by the bank. The fraudster deposits cash into the account, immediately withdraws the funds and then conducts a transfer to another bank account all before banking system records the initial cash deposit. This process is continued across multiple accounts to maintain the illusion of available funds.

3. **Credit Card Kiting:**
   This involves using multiple credit cards to pay off each other's balances without having the actual funds to settle the debt. The individual uses one card to make a payment on another card, continuously rotating the balances to keep accounts from defaulting.

HOW IT OCCURS

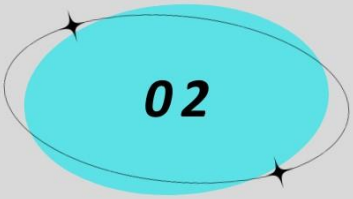


MECHANICS OF KITING



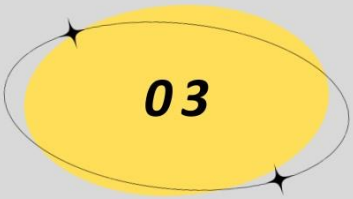
ACCOUNT OPENING:

The fraudster opens multiple bank accounts, typically at different banks or colludes with a network of individuals to open bank accounts either at the same bank or at different banks.



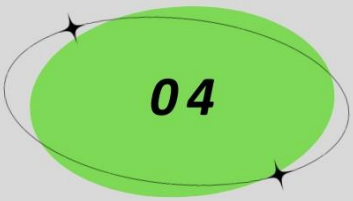
INITIAL DEPOSIT:

A deposit is made to the account. This is usually in the form of a cash deposit or bank transfer.



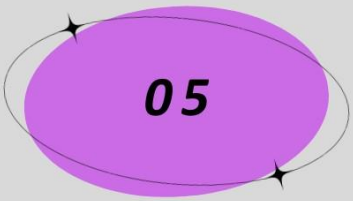
FUNDS WITHDRAWAL:

The funds are immediately withdrawn either via a cash withdrawal or bank transfer to another account held by the fraudster or to an account in the name of an individual who is colluding with the fraudster. This initiates the float period where the funds are considered deposited but has not yet cleared.



ADDITIONAL TRANSACTIONS:

Before the aforementioned transactions clear, the fraudster immediately conducts an additional bank transfer to an account in the name of an individual who is colluding with the fraudster. This action leverages the float period, creating a cycle of artificial funds availability.



CYCLE CONTINUATION:

This process continues, with the fraudster or persons in collusion with the fraudster depositing and withdrawing funds between multiple accounts to keep them in a constant state of apparent solvency thereby taking advantage of the artificially inflated balances created by the kiting scheme.

SUSPICIOUS INDICATORS

The following list of suspicious indicators provides guidance to FIs and NRFIs in assessing transactions to determine whether there are reasonable grounds to suspect the occurrence of Kiting.

Suspicious Indicators Involving Kiting:

1. Frequent Deposits and Withdrawals: High frequency of deposits and withdrawals, especially when the amounts are similar and occur within short intervals.

2. Inconsistent Account Activity:

    a. Account balances that show large fluctuations within short periods, often without a clear business rationale.
    b. Significant deposits immediately followed by withdrawals of nearly the same amount.

3. Float Period Manipulation: Multiple deposits from different banks or different accounts timed to exploit the float period, often with no apparent legitimate reason.

4. Cross-Bank Transactions: Multiple accounts across different banks or within the same bank with frequent related transfers that seem to lack a business or personal rationale.

5. Unusual Account Relationships: Accounts with no apparent business purpose or relationship engaging in frequent transfers, especially between accounts held by the same individuals or entities.

RECOMMENDATIONS FOR CONSIDERATION BY FIs

The FIUTT proposes that FI's and NRFI's protect themselves by implementing mitigating measures and safeguard the integrity of the financial sector through the implementation of more stringent measures including:

- Educate staff about the risks and signs of kiting.
    - Awareness Programs: Conduct group wide regular training sessions for staff to raise awareness about the signs of kiting and the importance of vigilance.
    - Detailed Guidelines: Provide detailed guidelines and checklists to help staff identify and report suspicious activities related to kiting.
- Set strict limits on overdraft facilities and monitor for excessive use.
    - Limit Overdraft Amounts: Set strict limits on the amount that can be over drafted to minimize the potential loss from kiting.
    - Overdraft Alerts: Implement alerts for frequent or large overdrafts to detect potential kiting activity.

- Implement tighter controls on transaction processing times.
    - Extended Hold Periods: Enforce longer hold periods on deposits, especially for new accounts or accounts with unusual activity. This allows more time to verify the legitimacy of the deposits.
    - Real-Time Verification: Use real-time check verification systems to confirm the availability of funds before releasing them. This can help prevent the exploitation of the float period.
- Monitor accounts for unusual patterns of deposits and withdrawals.
    - Regular Account Reviews: Conduct regular reviews of accounts with high transaction volumes, frequent overdrafts, or other red flags.
    - Enhanced Due Diligence: Apply enhanced due diligence procedures for accounts exhibiting suspicious behaviour, such as requiring additional documentation or verification.

Financial Institutions and Non-Regulated Financial Institutions are reminded that any transaction/activity suspected to be fraudulent or related to money laundering 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: August 21, 2024
Financial Intelligence Unit of Trinidad and Tobago