

2023

**EMERGING TREND –
Fraudulent Merchant Settlement**



Financial Intelligence Branch

Financial Investigations Division

12/5/2023

Contents

Disclaimer 2

Purpose of this Typology Report 2

 General Information 2

 Intelligence Indicators..... 3

 Statistics..... 3

 Conclusion 4

Disclaimer

The Financial Intelligence Unit (FIU) of the Financial Investigations Division (FID) is issuing this **Typology Report** in accordance with Section 5(2)(b) of the Financial Investigations Division Act 2010, to Competent Authorities and to Nominated Officers of Financial and Designated Non-Financial Institutions.

The information shared is intended for **general information purposes only** as it relates to an emerging trend within Jamaica’s financial sector. Therefore, the information contained is for **general guidance**, especially for the regulated sector and **must not** be replicated, without the written authorization from the Designated Authority of the FID.

Purpose of this Typology Report

The purpose of this Typology Report is to:

- inform Reporting Entities regarding an emerging trend identified as **“fraudulent merchant or electronic draft capture (EDC) settlements”**; and
- assist Reporting Entities in identifying the indicators relating to **“fraudulent merchant (EDC) settlements”**;

In order to safeguard the financial system from the risks associated with **fraudulent merchant settlements**, the FIU recommends that Financial and Designated Non-Financial Institutions share the information contained with relevant staff members and exercise caution by adjusting your monitoring system and/ or “red flag” mechanisms of your AML framework to identify and stop transactions of this nature from being processed.

General Information

“Electronic Draft Capture” is an essential technology that facilitates the electronic payment of funds with the use of a card or a digital wallet. The EDC technology retrieves the customer’s banking information and captures the draft or the amount due. Once the funds are secured, the money transmits to the merchant’s account. Therefore, all business e-transactions are dependent on EDC¹.

Intelligence available disclosed that perpetrators’ accounts, mainly accounts with an associated POS merchant machine are being credited with fraudulent EDC payments from the settlement of their POS machine. This is being achieved through the processing of cards in **“offline mode”**, with some instances, cards being associated with international financial institutions.

Offline Card Processing is where a POS transaction is facilitated with the merchant having no internet, i.e. the merchant is **“offline”**. The cardholder account number and other data is

¹ <https://www.ebanx.com/en/resources/payments-explained/electronic-draft-capture-edc/>

encrypted and held in the payment processor until the merchant is back online and the merchant initiates the settlement of the POS machine.

Intelligence Indicators

The main indicators identified from the intelligence received entailed the following:

1. Account used as a repository for fraudulent credit card transaction with an international card processed in **“offline mode”** with amount credited to account via EDC settlement;
2. Credit card transaction processed in **“offline mode”** and later confirmed fraudulent, which was credited to the perpetrators account via EDC settlement;
3. Merchant activities deemed fraudulent on the merchant settlement portal, with international credit cards processed deemed to be fraudulent that is not customary with the usual activities of the perpetrators’ accounts.

Summary of the Intelligence Indicators:	
Suspected Offence	Fraud
Type	EDC Settlement Fraud (Credit Card processed in offline mode)
Sector	Financial Institutions (<i>Deposit taking institutions</i>)
Customer Type	Business/Entity
Channel	POS/ EDC Technology (Electronic)
Jurisdiction	Foreign; Local

Statistics

For the period May to September 2023, the FID has identified twenty-nine (29) incidences of **“fraudulent merchant (EDC) settlements”** that contained a total of one hundred and fourteen (114) **processed transactions** totaling approximately J\$700M. Financial institutions would have reported the detection and recovery of majority of the fraudulent proceeds. However, at least 11%, i.e. approximately J\$79M was irrecoverable due to either through the perpetrators immediately conducting:

1. electronic transfers of these fraudulent funds to other perpetrators at other financial institutions;
2. Cash withdrawals from the ATM; and
3. POS transactions with other merchants.

Tran. Mode	Tran. Count	J\$ Value
EDC Settlements	114	699,630,440.31
Electronic Transfers (<i>incl. RTGS, Account to Account Transfers</i>)	73	(76,641,517.73)
Cash Withdrawal	3	(2,800,000.00)
Net Diff.	190	620,188,922.60

The **“fraudulent merchant (EDC) settlements”** transactions captured at least twenty-four (24) different perpetrators with several international credit cards processed in **“offline mode”**.

The perpetrators, were mainly businesses with assigned POS Merchant Machines that are involved in several different industries inclusive of;

- ✓ Hardware
- ✓ Motor Vehicle Sales
- ✓ Wholesales/ Variety Stores
- ✓ Pharmaceutical
- ✓ Electronic Sales & Repairs
- ✓ Consultancy services

Conclusion

Reporting Entities need to exercise due diligence in the issuance of POS merchant machines to businesses. Based on the risk profile of the client the necessary mitigating measures or red flags must be implemented to detect the possible abuse of the service granted. Therefore, the risk profile must include:

1. Geographical location
2. Product offerings
3. Target market
4. Analyze financials and cash flow statements to estimate average daily sales