2024

EMERGING TREND – REFUND & DOUBLE REFUND (CHARGEBACK) FRAUD

Financial Intelligence Branch

Financial Investigations Division

7/23/2024

Contents

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 involving e-commerce identified as **"refund fraud"** and **"double refund (chargeback) fraud".** Note the **"double refund (chargeback) fraud"** reports specifically targeted one of the leading e-commerce platform during 2023;
- assist Reporting Entities in identifying the indicators or observed techniques or trends relating to **"refund fraud"** and **"double refund (chargeback) fraud";**
- inform Compliance Officers of observed techniques and trends relating to the overseas merchants that appear to be targeted;

In order to safeguard the financial system from the risks associated with **"refund fraud"** and **"double refund (chargeback) fraud",** the FIU recommends that Financial and Designated Non-Financial Institutions share the information contained with relevant staff members. Ensure the necessary caution is exercised by adjusting the monitoring system and/ or "red flag" mechanisms of your AML framework to identify and stop transactions of this nature from being processed.

General Information

"Refund Fraud" is a type of e-commerce fraud that is attempted against an e-commerce business/ store/ platform. Intelligence available disclosed two (2) methods of this fraud:

1. The perpetrators' accounts were credited with funds from overseas merchants. There is however, no evidence of any online debit/ credit card purchase being initiated from the perpetrators' debit/ credit card accounts. The FIU and/ or the reporting entities have yet to determine and/ or identify the basis for which these **"refunds"** from the overseas merchants were directed to the perpetrators' accounts; considering, the online transactions were never initiated from the perpetrators' accounts. Hence, the source of funds used to initiate the transactions remains anonymous.

2. The perpetrators' accounts were credited with both a refund and a chargeback for a single transaction. This usually occurs when the merchant refunds a customer while the customer simultaneously initiates a chargeback through their bank. Based on the volume of transactions reported it appears intentional and is referred to as **"double refund (chargeback) fraud",** where bad actors increasingly leverage the double refund chargeback as a tool for scamming merchants[1].

Open Source Explanation

The following description of **"refund fraud"** addresses the means by which the e-commerce transactions were possibly initiated and why no transactional history with the overseas merchants were identified on their clients', the fraudsters', accounts:

> *"In **refund fraud**, the fraudster uses stolen credit card credentials to make an online purchase, and then contacts the e-commerce store to request a reimbursement.*
>
> *A common refund tactic is for the fraudster to deliberately make an excess payment, then request a **refund** for the excess amount while requesting that the money be sent **via an alternative method** (e.g. by claiming the credit card was closed). This way, the fraudster can receive the **"excess" amount** without having **the original card charge refunded**, which could result in a chargeback when the original owner of the credit card makes their disputes."*
>
> *https://datadome.co/learning-center/7-types-of-ecommerce-fraud-how-to-prevent-them/*
>
> *Similar description can be viewed on https://thegood.com/insights/ecommerce-fraud/*

The following extract from an online article entitled ***"Double Refund Chargebacks, Preventing Double Refunds: before & After a Dispute"*** dated December 13, 2023, highlighted the following:

[1] chargebacks911.com/double-refund-chargebacks/#:~:text=A%20double%20refund%20chargeback%20occurs%20when%20a%20customer%20receives%20a,refunds%20for%20a%20single%20purchase.

*"A **double refund chargeback** can happen inadvertently. However, an increasing number of consumers are manipulating the chargeback process and are refunded twice for the same transaction. Once via the refund process, and once via the chargeback process."* Noting that the *"refund process is initiated by the merchant directly to the customer…, while a chargeback is a forced transaction reversal initiated by the customer's bank or credit card issuer, often due to a dispute or unauthorized charge claim."*

Two (2) primary ways this can occur:

1. Chargeback Filed After Issuing A Refund – the consumer contacts the merchant requesting a refund. The merchant honor the request. The funds, however, do not show in the customer's account when expected. The customer files a chargeback, assuming the merchant ignored or denied the refund request. Both the chargeback and the refund both are processed.

2. Chargeback Filed Before the Refund is Issued – the consumer contacts the bank and initiated a dispute. The same customer then contacts the merchant and requests a refund. The merchant in order to avoid a chargeback, issues the refund without the knowledge that the customer had already filed a dispute with their bank.

https://chargebacks911.com/double-refund- https://chargebacks911.com/double-refund-chargebacks/#:~:text=A%20double%20refund%20chargeback%20occurs%20when%20a%20customer%20receives%20a,refunds%20for%20a%20single%20purchase.

Intelligence Indicators

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

Refund Fraud:

Summary of the Intelligence Indicators:	
Suspected Offence	Fraud
Type	E-commerce Fraud – Refund Fraud
Sector	Financial Institutions *(Deposit taking institutions)*
Customer Type	Individual & Online Merchants
Channel	Electronic – Debit/Credit Card Online POS
Jurisdiction	Foreign; Local

1. Unusual debit card refunds reflected on clients' accounts;
2. No debit/ credit card purchase reflected on clients' accounts;
3. Multiple deposits to accounts said to be ***"refunds"*** from overseas suppliers;
4. Fraudulent refunds/ fraudulent merchant refunds/ fraudulent electronic refunds from various merchants located overseas; and
5. Refunds credited to accounts were immediately withdrawn by way of electronic transfers, ABM cash withdrawals and point of sale transactions.

Double Refund (Chargeback) Fraud:

Summary of the Intelligence Indicators:	
Suspected Offence	Fraud
Type	E-commerce Fraud – Double Refund Chargeback Fraud
Sector	Financial Institutions *(Deposit taking institutions)*
Customer Type	Individual & Online Merchants
Channel	Electronic – Debit/Credit Card Online POS
Jurisdiction	Foreign; Local

1. Multiple payments made to merchant followed by duplicated reversal/refunds for the original transactions.
2. Online payments to merchant followed by POS reversals of the payments and then refunded amounts credited to the account from the merchant.
3. Refunds all came from one (1) merchant, which appears to be duplicated refunds for cancelled POS purchases.
4. Account used to receive fraudulent credits in the form of refunds from a merchant that appear to be duplicated refunds for cancelled POS purchases.
5. Transactions on the account reflect POS payments to a merchant that were cancelled/ reversed on the same day i.e. debit with a matching credit. Then the same value cancelled/ reversed again and credited to the account at least a day later.

Statistics

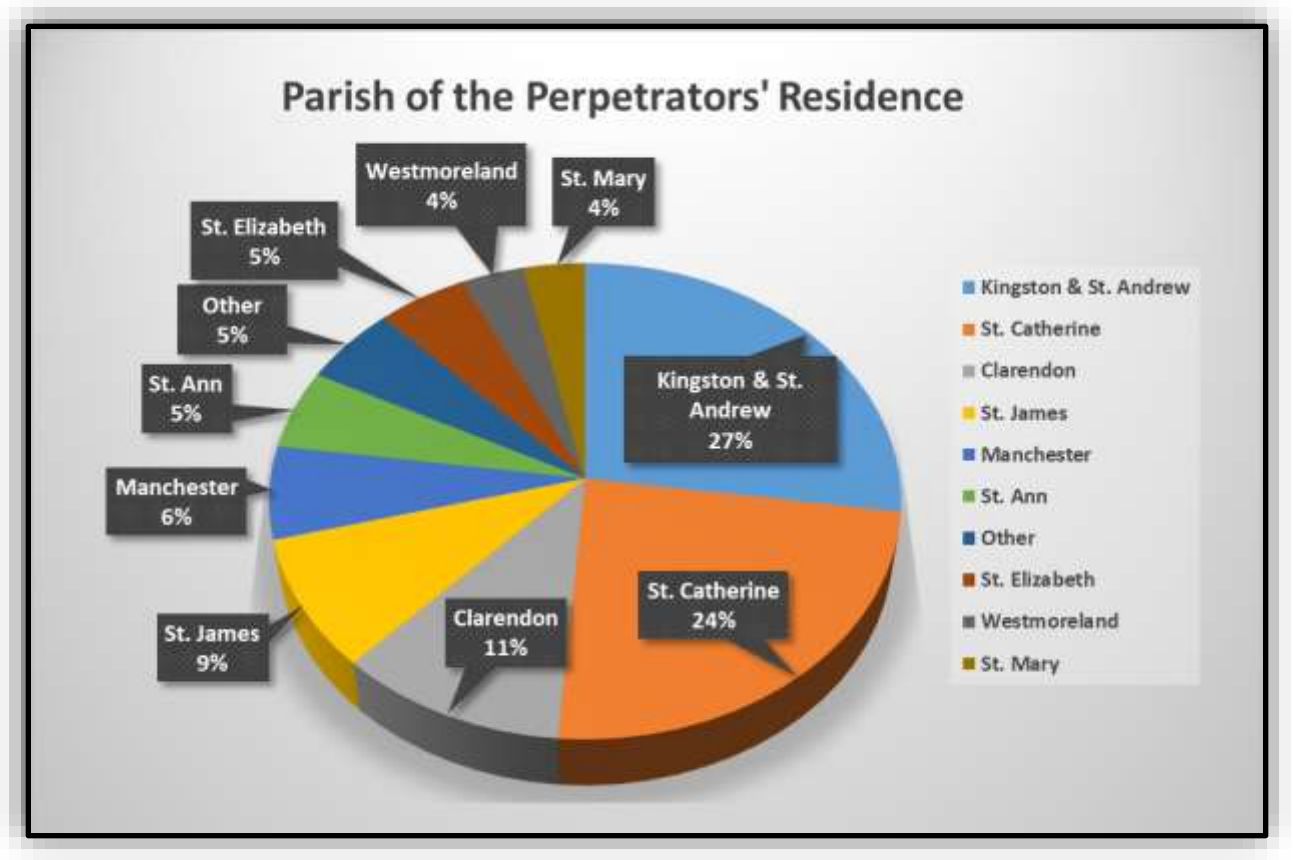
For the period January to December 2023, the FID has identified two hundred and ninety-eight (298) incidences of the **"refund fraud"** and **"double refund (chargeback) fraud"** that contained a total of three thousand , three hundred and fifteen (3,315) **processed transactions** and fifty-nine (59) **attempted transactions**. The monetary value of these fraudulent transactions, inclusive of **attempted transactions** was approximately J$245M.

Sector	Report Count	Tran. Count	J$ Value
Commercial Bank	290	2,405	124,286,024.00
Credit Union	8	61	48,226,301.94
Other	-	908	72,298,236.50
Grand Total	**298**	**3,374**	**244,810,562.44**

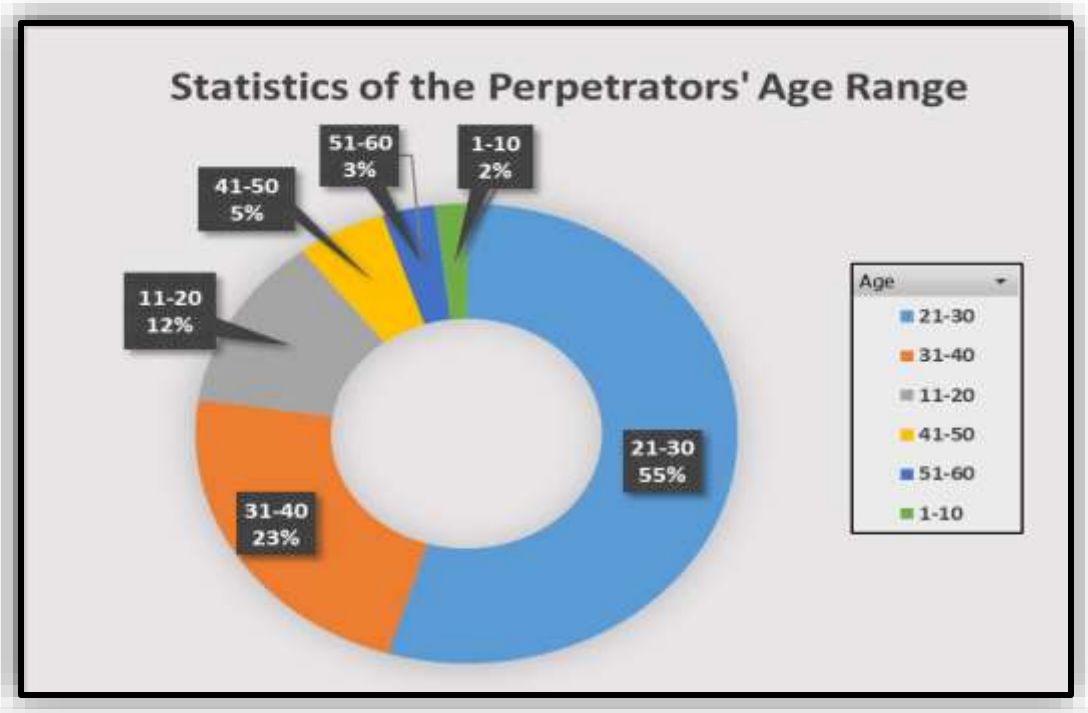
The **"refund fraud"** and **"double refund (chargeback) fraud"** transactions captured at least three hundred and sixteen (316) different perpetrators whom targeted at least one hundred and ninety-seven (197) different overseas merchants.

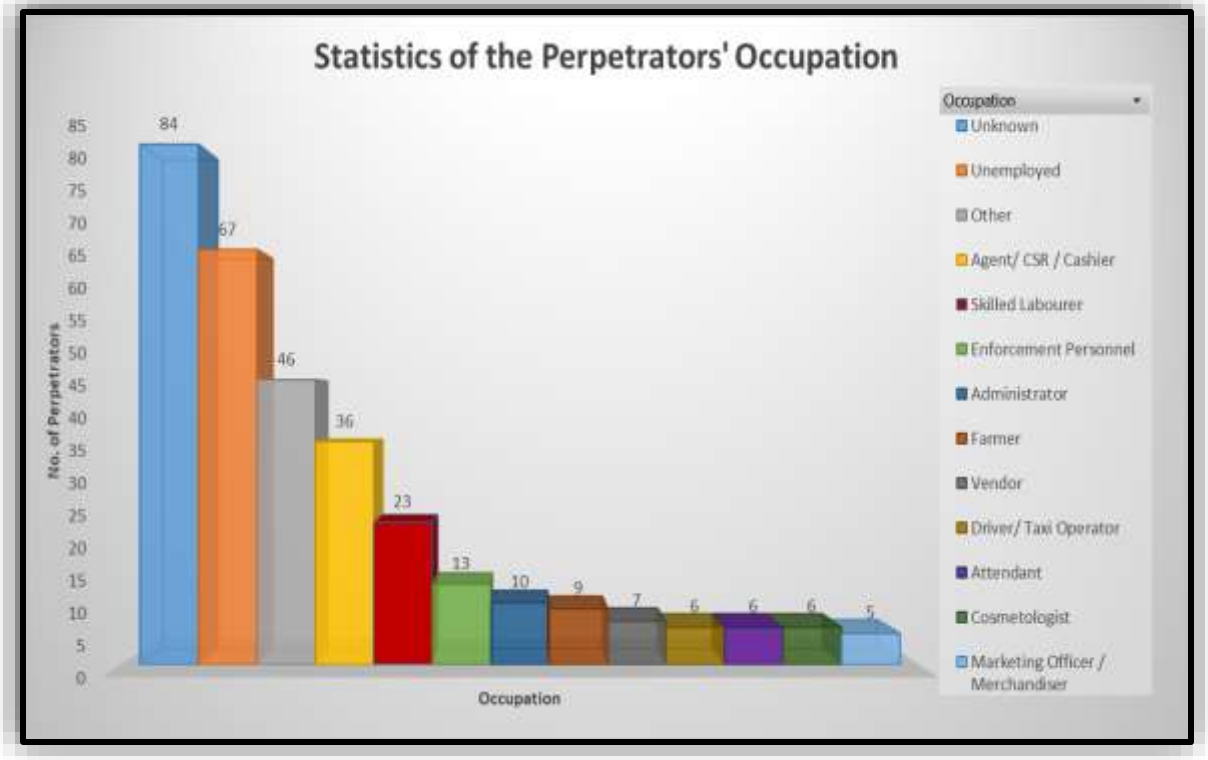
Profile of the Perpetrators

All the perpetrators were Jamaican nationals residing across the fourteen (14) parishes, with majority of the addresses being in the Kingston & St. Andrew and St. Catherine parishes.



The 21 – 30 age group accounted for approximately 55% (i.e. 174 perpetrators) of the total perpetrators who engaged in the **"refund fraud"** and **"double refund (chargeback) fraud"** scheme, with the occupations being mostly low income earning positions and approximately 21% stated to be unemployed. See below graphical representation of the statistics:





Conclusion

Based on the social profile of the perpetrators that are involved and the volume of overseas merchants, Financial and Designated Non-Financial Institution must assess their clients' transactions/activities to determine whether there are reasonable grounds to suspect the occurrence of **"refund fraud"** and **"double refund (chargeback) fraud".** Where the analysis gives rise to the suspicion of **"refund fraud"** and **"double refund (chargeback) fraud"** then a disclosure should be made to the Designated Authority – FID.

The methods described with these emerging trends provide a potential avenue for these funds to be laundered as observed with one (1) of the perpetrators reported as described below:

Intelligence Dissemination:

Client A was reported by two (2) financial institutions in 2023 disclosing the following:

"Account X was being used to receive fraudulent credits in the form of refunds from a particular e-commerce merchant. Based on the review, the transactions appear to be duplicated refunds for cancelled online purchases.

The financial institution observed several transfer of the funds from Account X to Client A's account at another financial institution (Account Y). The funds accumulated in Account Y from transfers of the fraudulent funds in Account X was then used to open an investment policy.

Client A, a Used Car Salesperson, indicated the source of funds accumulated in Account Y were from the purchase and resale of a motor vehicle."

Further review of Client A, also confirmed several asset acquisition within the same timeframe of financial institutions report on the client's activities.

The FIU prepared an intelligence report with the view that the combined activities reported were highly indicative of money laundering and disseminated to the investigative officers of the FID.

Regulated entities, therefore, must exercise caution by:

- ✓ Adjusting their monitoring system and/ or "red flag" mechanisms of their AML framework to identify and stop transactions of this nature from being processed;
- ✓ Consider extending the timeframe for effecting a customer's dispute regarding e-commerce transaction(s) with their clients. As based on reports and open source explanation, perpetrators have discovered a means to defraud both merchant and bank simultaneously.

- ✓ Monitoring the social media space to determine whether their clients are being solicited to partake in fraudulent schemes requiring the sharing of their assigned debit/credit card details. The intelligence had provided an Instagram account with the handle ***'@visacardholder'*** soliciting persons who are in possession of MasterCards and/ or VISA cards.
- ✓ Educating and being responsive to social media activities that appear to be targeting their clients and/ services offered.
- ✓ Obtaining and verifying customers details provided when onboarding, inclusive of occupation and place of employment.
- ✓ Ensuring provisions are in place to minimize payment of fraudulent proceeds to the perpetrators.
- ✓ Ensuring staff members are kept informed and are made aware of emerging trends used by criminals to launder money, through continuous training and/ or compliance newsletters.

Overall, ensure that the appropriate policies, internal controls and reporting mechanisms are in place to guide management and staff in executing their roles in detecting, deterring and/ or reporting the activities of clients that resembles any method of money laundering and/ or involvement in financial crimes.