# Digital Forensic Report

By: Trevor Hofmann

Date: February 17, 2024

## Summary of Analysis

Objective 1: Perform an audit to find fraud using SQL.

Mark Moore made 74 returns over the average price of all returns. It is over double the next closes employee, Charles Whitehead, with 33 returns that are over the average price of all returns.

Mark Moore made 46 returns to credit card number 2703144240071235 and 22 returns to 40077653923591. No other employee had repeated returns to the same credit card number.

Objective 2: Perform an audit to find improper procedure violations using SQL.

Mark Moore has 68 returns compared to the only other two employees that made returns in violation of store policies is 4 and 13 makes him an obvious outlier. It is a business policy to only give money back on returns to someone without a receipt only on gift card. This means any returns are made this way are in violation of the business policies. Joseph Smith with only 4 could be accidental and Anthony West Jr. with 13 returns could be sign of fraud but there is not enough instances to draw that conclusion.

Summary: This evidence supports the claim that Mark Moore committed fraud.

## Objectives

1. Perform an audit to find fraud using SQL.
2. Perform an audit to find improper procedure violations using SQL.

## Chain of Custody

Using the SHA-265 checksum to generate a hash we have verified the file has not been changed while in custody.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Table 1: Chain of Custody | | | | |
| File Name | Date of the file | Date Received | Original Hash | Post Hash |
| customer\_returns\_simulated\_data.db | 02-17-2024 | 02-17-2024 | EF767EA6136EB0146A636D3BEF791AA78D2C45891174CC87CB1F8EFA3214DD8E | EF767EA6136EB0146A636D3BEF791AA78D2C45891174CC87CB1F8EFA3214DD8E |

## Methods and Tools Used

Windows PowerShell

# Specify the path to the directory containing PNG files

$directoryPath = "C:\Users\BlueBravo\OneDrive - West Texas A and M University\Masters\SP2024\CIDM 6356 DF\Week 6\customer\_returns\_simulated\_data.db"

$hash = Get-FileHash -Path $directoryPath

Write-Host "$hash"

SQL

SQLite

Review Policy

Company Policy Regarding Customer Returns these are the key points and red flags to search for in the data.

* 1. Key Points:
     1. Find returns without receipts and where funds were returned to a debit/credit card.
     2. Find returns without receipts and where funds were returned to a gift card.
     3. Find instances where an employee-initiated return for any inventory items, especially if they were quickly returned to the shelf.
  2. Red Flags:
     1. Frequent returns without receipts, especially if they involve high-value items.
     2. Employees initiate returns and immediately place the refunded items back on the shelf.
     3. Unusual patterns in return dates or return prices.

Build Query

1. Query to search instances where there is a return without receipt and without giving a gift card.

*SELECT employee."EmployeeID", employee."Name" AS "EmployeeName", COUNT(returns."ReturnId") AS "ReturnCount"*

*FROM employee*

*LEFT JOIN returns ON employee."EmployeeID" = returns."EmployeeID"*

*WHERE returns."ReceiptId" IS NULL AND returns."IsReceiptPresent" = "False" AND returns."GiftCardNumber" IS NULL*

*GROUP BY employee."EmployeeID", employee."Name";WHERE "EmployeeID" is "7857";*

1. Query to search for and count all returns over the average price of returns

*WITH AverageReturn AS (*

*SELECT AVG("ReturnPrice") AS "AverageReturnPrice"*

*FROM returns*

*WHERE "ReturnPrice" IS NOT NULL*

*)*

*SELECT employee."EmployeeID", employee."Name" AS "EmployeeName", COUNT(returns."ReturnId") AS "HighValueReturnCount"*

*FROM employee*

*JOIN returns ON employee."EmployeeID" = returns."EmployeeID"*

*JOIN AverageReturn ON 1=1*

*WHERE returns."ReturnPrice" > AverageReturn."AverageReturnPrice"*

*GROUP BY employee."EmployeeID", employee."Name"*

*ORDER BY "HighValueReturnCount" DESC*

*LIMIT 5;*

1. Query to count each time an employeeID and CreditCarNum are used.

*SELECT employee."EmployeeID", employee."Name" AS "EmployeeName", returns."CreditCardNum", COUNT(returns."ReturnId") AS "UsageCount"*

*FROM employee*

*JOIN returns ON employee."EmployeeID" = returns."EmployeeID"*

*WHERE returns."EmployeeID" IS NOT NULL AND returns."CreditCardNum" IS NOT NULL*

*GROUP BY employee."EmployeeID", employee."Name", returns."CreditCardNum"*

*ORDER BY "UsageCount" DESC*

*LIMIT 10;*

Run Query

After running the queries this is the resulting data:

Query 1 results:

|  |  |  |
| --- | --- | --- |
| Table 2: Query 1 Results | | |
| EmployeeID | EmployeeName | ReturnCount |
| 3277 | Joseph Smith | 13 |
| 7857 | Mark Moore | 68 |
| 9663 | Anthony West Jr. | 4 |

Quary 2 results:

|  |  |  |
| --- | --- | --- |
| Table 3: Query 2 Results | | |
| EmployeeID | EmployeeName | HighValueReturnCount |
| 7857 | Mark Moore | 74 |
| 7795 | Charles Whitehead | 33 |
| 2687 | Daniel Johnson | 31 |
| 1085 | Selena Barker | 30 |
| 3277 | Joseph Smith | 30 |

Quary 3 results:

|  |  |  |  |
| --- | --- | --- | --- |
| Table 4: Query 3 Results | | | |
| EmployeeID | EmployeeName | CreditCardNum | UsageCount |
| 7857 | Mark Moore | 2703144240071235 | 46 |
| 7857 | Mark Moore | 40077653923591 | 22 |
| 259 | Marcus Gilbert | 060401492461 | 1 |
| 259 | Marcus Gilbert | 180093496264919 | 1 |
| 259 | Marcus Gilbert | 213113075160246 | 1 |

## Relevant Findings

Query 1

Mark Moore employee number 7857 had 68 returns.

Mark Moore has significantly more returns than any other employee making returns without receipt and without giving a gift card. This type of return is against policy.

Since it is against policy any returns this way are a sign of a problem. Because of this Joseph Smith and Anthony West Jr. are in violation. Joseph Smith with only 4 could be accidental and Anthony West Jr. with 13 returns could be sign of fraud but there is not enough instances to draw that conclusion. Mark Moore having 68 returns is such a significant outlier that it must be more than negligence.

Query 2

Mark Moore made 74 returns over the average price of returns. It is over double the next closes employee Charles Whitehead with 33 returns over the average price of returns.

Query 3

Mark Moore made 46 returns to credit card number 2703144240071235 and 22 returns to 40077653923591. No other employee had repeated returns to the same credit card number.

Summary

All three queries repeatedly show that Mark Moore is making returns that are obvious red flags. These findings support our claim that Mark Moore is committing fraud.