**Digital Forensics**

**Title –** Detecting Retail Employee Fraud

**Author –** Miguel Sanchez

**Executive Summary**

The focus of our forensic analysis team was to identify violations of a retail company's return policy and detect potentially fraudulent activities within sales/returns transactional data. The rationale is that consistent policy violations, while not conclusively fraudulent, often reveal trends that could indicate fraudulent behavior, such as repeated use of the same credit card for returns without receipts. Our fraud detection team utilized Structured Query Language (SQL)Lite, this tool has been used for identifying accounting fraud and can be leveraged to analyze data irregularities. Through a series of SQL queries, we identified 85 instances of returns issued to a credit card without a receipt, a violation of company returns policy 5-a. In particular, Employee ID 7857 (Mark Moore) executed a disproportionate number of these transactions, amounting to 68 returns totaling $4,172.98, denoting a high likelihood of fraudulent conduct. Further analysis revealed a pattern of returns to two specific credit card numbers associated with Moore, which blatantly contrasts with the behavior of other employees, such as Employee ID 3277, John Mason, whose returns were dispersed across different cards. The investigation revealed meaningful evidence of fraudulent activity by Mark Moore, accounting for 34.7% of all returns in the analysis period. This pattern of behavior, coupled with the violation of return policies, imposes immediate and appropriate legal action to mitigate further financial loss and uphold the retail organization's integrity. Moreover, our analysis highlighted two employees, including John Mason (Employee ID 3277) and Anthony West Jr (Employee ID 9663) have violated the company’s return policy.

**Objectives**

The goal of this analysis is to 1) identify potential violations of the company’s return policy and 2 to detect any fraudulent activities that may be occurring. While return policy violations may not be 100% fraudulent it may be able to illuminate on trends that humans tend to exhibit (i.e same credit card used for a return, lack of receipt being present etc.). When a fraudster gets away with an illegal activity the initial few times (two to three) the confidence of the fraudster begins to increase, and they tend to get sloppy with their activities. Our goal will be to identify these potentially fraudulent activities and test our SQL models to determine “one-off”, “honest mistakes” from true fraudulent examples. After thorough review and analysis of the database provided, we have determined that Mark Moore has completed fraud by completing a total of 68 transactions for a total amount of $4,172.98.

**Chain of Custody**

An extract of the retail chain database was provided was downloaded on February 24th, 2024.

The SHA-256 Checksum hash number is 36821523F51EE71F48D50813CB9F5B979C9111745133C95F2348830C9BD56B71 and file name is “customer\_returns\_simulated\_data.db”.

**Methods and Tools Used**

When identifying the best approach to tackle this investigation our fraud detection team decided to use a widely used method to identify accounting fraud, Structured Query Language “SQL”. The fraud investigation community use various tools at their disposal to identify potentially fraudulent activities and SQL is by far one of the most common tools used by organizations trying to identify accounting fraud.

SQL Code Used for Investigation

**First SQL Analysis – “Number of Returns without Receipt but Return method via Credit Card”**

SELECT employee.EmployeeId, employee.Name,

COUNT(\*) AS NumberOfReturns

FROM employee

INNER JOIN returns ON employee.EmployeeId = returns.EmployeeId

WHERE returns.IsReceiptPresent = 'False'

AND returns.CreditCardNum IS NOT NULL

GROUP BY employee.EmployeeId, employee.Name

ORDER BY NumberOfReturns DESC;

**Second SQL Analysis – “Count of EmployeeID returns completed from population of 85 return policy violations”**

SELECT employee.EmployeeId, employee.Name,

COUNT(\*) AS NumberOfReturns,

SUM(returns.ReturnPrice) AS TotalReturnPrice

FROM employee

INNER JOIN returns ON employee.EmployeeId = returns.EmployeeId

WHERE returns.IsReceiptPresent = 'False'

AND returns.CreditCardNum IS NOT NULL

GROUP BY employee.EmployeeId, employee.Name

ORDER BY ReturnPrice ASC

**Third SQL Analysis – “Count of returns for each EmployeeId and Credit Card Number”**

SELECT employee.EmployeeId, employee.Name,returns.CreditCardNum,

COUNT(\*) AS CountOfReturns

FROM employee

INNER JOIN returns ON employee.EmployeeId = returns.EmployeeId

WHERE employee.Name = 'Mark Moore'

AND returns.IsReceiptPresent = 'False'

AND returns.CreditCardNum IS NOT NULL

GROUP BY employee.EmployeeId, returns.CreditCardNum;

**Fourth SQL Analysis – “Count of returns for each EmployeeId where a return was completed and receipt is not present”**

SELECT employee.EmployeeId, employee.Name,

COUNT(\*) AS CountOfReturns

FROM employee

INNER JOIN returns ON employee.EmployeeId = returns.EmployeeId

WHERE returns.IsReceiptPresent = 'False'

GROUP BY employee.EmployeeId

ORDER BY CountOfReturns DESC;

**Relevant Findings**

**First SQL Analysis – “Number of Returns without Receipt but Return method via Credit Card.”**

When running this initial SQL analysis, we identified that there are 85 return policy violations where a return was completed without a Receipt and the return was issued in the form of a credit card. This is a clear violation of company return policy 5-a. Now all of these may not truly be fraudulent, therefore an additional layer of analysis must be added.

*Figure 1*

A screenshot of a phone

Description automatically generated

*Count of Employee Returns to a credit card without a receipt present.*

**Second SQL Analysis – “Count of EmployeeID returns completed from population of 85 return policy violations.”**

The second SQL analysis we noticed there was one employee with a large count of returns, “68” to be exact. Employee ID 7857 “Mark Moore” was responsible for 80% of all returns that were completed without a receipt and issued the return on a credit card. The second highest offender with 13 returns was Employee ID 3277 “John Mason” (but these seem less likely to be fraudulent, additional analysis of both populations is needed. Furthermore, Anthony West Jr (Employee ID 9663) was also one of the policy violators. Our findings suggest that these actions may not have been of malicious intent nor fraudulent (additional investigation steps would be necessary to confirm). This should be treated as a valuable training opportunity to ensure that all team members are fully compliant with the company's return policies.

*Figure 2*

A screenshot of a number of numbers

Description automatically generated

*Count of returns and Total Return Price for completed returns from population of 85 return policy violations.*

**Third SQL Analysis – “Count of returns for ‘Mark Moore’ and Credit Card Number”**

Our third SQL query further broke down the dataset at a more granular level. This query helps group the population by both EmployeeId and Credit Card Number. This breakdown allows us to identify that the 13 instances for employee “John Mason” (EmployeeID 3277) were sporadic returns and all of them were to different credit cards. As for “Mark Moore” (EmployeeID 7857) there are 46 and 22 returns completed to credit card numbers \*\*\*\*\*\*\*\*\*\*\*\*1235 and \*\*\*\*\*\*\*\*\*\*3591, respectively. These two credit cards being used for returns is exhibiting signs of a high risk of fraud.

*Figure 3*

A screenshot of a credit card

Description automatically generated

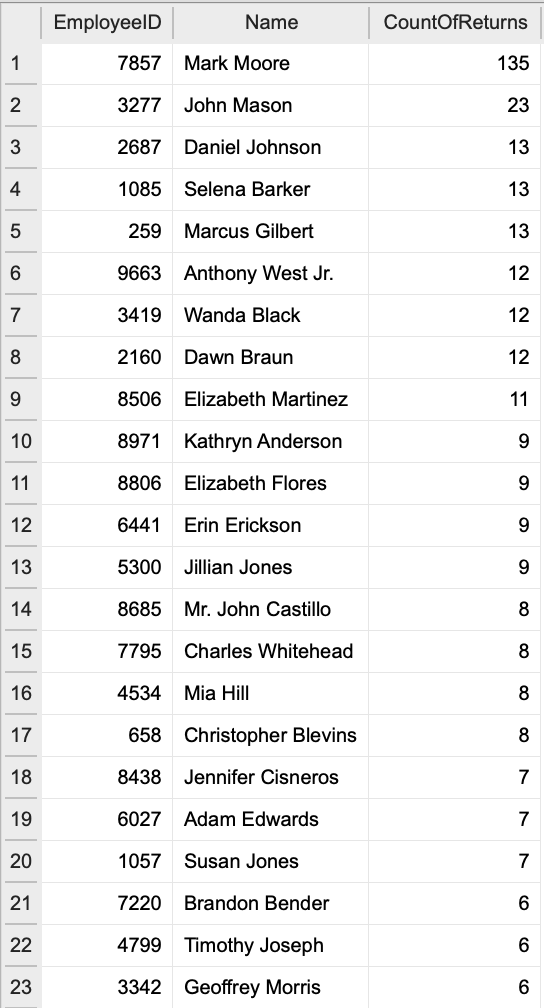
*Count of returns for ‘Mark Moore’ and Credit Card Number*

**Fourth SQL Analysis – “Count of returns for each EmployeeId where a return was completed, and receipt is not present.”**

This query provides a count of all returns completed (regardless if the receipt is present or not) for each employee. This allows us to see the trends of the column we titled as “CountOfReturns”. By drilling down on this data, we have identified that the same culprit is responsible for 135 returns (EmployeeID 7857, “Mark Moore”). Mark Moore has 122 more returns that the second highest returns by employee which is 13.

Additional research is required for this population of 135 (excluding the 68 without a receipt being present, since our team identified this population already) and identify the gift cards and credit cards that were used for these returns. Mark Moore is single-handedly responsible for 34.7% of all returns for the retail chain for the time-period we are investigating. We can further break down this data to bring in the sum of the total return price for this population and identify the impact to the retail organization. Our team has identified fraud that has taken place by EmployeeID 7857, Mark Moore and corrective/legal action should be taken to protect the integrity of the retail organization.

*Figure 4*



*Count of returns for each Employee where a return was completed, and a receipt was not present.*