Incident Report: Financial Fraud and Theft Investigation
Case ID: REMI-2024-0453
Report Date: April 10, 2024
Prepared by: REMI System – AI-Generated Summary for Financial Auditors and Compliance Officers

Subject: Investigation into Unauthorized Financial Transfers and Asset Misappropriation

Summary of Events

On **March 25, 2024**, a pattern of unauthorized high-value transactions was detected involving **Account Number 394827569** at **MetroStar Bank**, headquartered in **Chicago, IL**. Initial data analysis flagged suspicious fund movements from this account to several foreign and domestic accounts, raising suspicions of coordinated financial theft.

The primary suspect, identified as **Lucas Finley** (User ID: lfinley), holds a managerial position in **Skyline Holdings LLC**'s finance department. Finley had authorized access to several high-level accounts, including the one in question, but data analysis shows his access patterns significantly deviated from standard protocol.

Chain of Events

1. **March 24, 2024 – Initial Access**
   Logs indicate that **Lucas Finley** accessed **Account Number 394827569** outside regular business hours, initiating the login from a new IP address located in **Los Angeles, CA**. Geo-location data further reveals that multiple subsequent access attempts were conducted from **Toronto, Canada** over the next 24 hours, suggesting potential VPN usage or remote collaboration.
2. **March 25, 2024 – Suspicious Transactions Initiated**
   At **2:15 PM**, Finley authorized a wire transfer of **$250,000** to **Account Number 128746519** under the name **BlueBay Consultants Ltd.**, an entity flagged for previous suspicious activity. BlueBay Consultants, based in **Nassau, Bahamas**, is known for associations with **Redstone Group**, a suspected shell corporation linked to several cases of offshore tax evasion and laundering operations.
3. **March 26, 2024 – Escalation of Fund Transfers**
   By the following morning, Finley had conducted four additional transactions, each to different accounts under varying names, including **Emerald Financials** and **Northern**

Holdings LLC, both based in **Hong Kong**. Each transaction, roughly **$100,000** to **$200,000**, lacked standard documentation and deviated from Skyline Holdings' vendor approval list. Finley, leveraging his managerial privileges, bypassed the typical multi-tiered approval process, thereby avoiding internal scrutiny.

4. **March 27, 2024 – Involvement of Secondary Personnel**
   Anomalies in the transaction logs indicate that **Amy Larson** (User ID: alars) from Skyline Holdings' accounting team granted Finley temporary administrative overrides on multiple accounts, under the pretense of "urgent audit reconciliations." Larson, based in **New York, NY**, has no documented history of high-level authorizations, raising suspicions of possible collusion or unintentional compliance.
5. **March 28, 2024 – Detection of Data Access Anomalies**
   REMI detected Finley accessing confidential financial records titled **"Strategic_Financial_Reserves_March2024.xlsx"** on **Workstation-F01**, located in **Skyline Holdings' Los Angeles branch**. Metadata analysis revealed multiple attempts to download the file onto an unauthorized external device, indicating potential intent to exfiltrate sensitive financial information. Further, Larson's user ID shows that she granted access to the document shortly before it was downloaded, raising questions about her role in facilitating the data breach.
6. **March 29, 2024 – Termination of Transactions and User Access**
   After flagging these events, the compliance team at Skyline Holdings, informed by REMI's early alerts, locked down both Finley's and Larson's access. Immediate freeze orders were placed on accounts connected to **BlueBay Consultants Ltd.**, **Emerald Financials**, and **Northern Holdings LLC**.

Summary of Findings

Primary Suspect:

- **Name:** Lucas Finley
- **Role:** Finance Manager, Skyline Holdings LLC
- **Location:** Los Angeles, CA

Finley conducted unauthorized high-value transactions and attempted to exfiltrate confidential data. His access patterns, including the times and geo-locations of logins, were highly irregular, and he used his managerial privileges to bypass security protocols.

Additional Involved Personnel:

- **Name:** Amy Larson
- **Role:** Accountant, Skyline Holdings LLC
- **Location:** New York, NY

Larson provided Finley with temporary administrative overrides and access to sensitive documents, suggesting either complicity or oversight failure in compliance processes.

Involved Organizations and Accounts:

- **BlueBay Consultants Ltd.** – Nassau, Bahamas
- **Emerald Financials** – Hong Kong
- **Northern Holdings LLC** – Hong Kong
- **MetroStar Bank Account Numbers Involved:**
  - **394827569** (Primary account for unauthorized transactions)
  - **128746519** (Destination account in the Bahamas for first transaction)

Conclusion

The sequence of events, including unauthorized access, geo-location changes, structured fund transfers, and involvement of offshore accounts, points to a coordinated financial crime scheme. Lucas Finley appears to have initiated the fraud with possible assistance from Amy Larson, who facilitated unauthorized permissions.

The evidence suggests that Finley exploited his managerial access to initiate high-value transfers to entities with known affiliations to offshore laundering operations. With Larson's assistance, Finley circumvented internal controls, making Skyline Holdings vulnerable to further unauthorized access and financial misappropriation.

Actionable Recommendations:

1. **Freeze all associated accounts** to prevent further fund transfers.
2. **Audit all administrative overrides and high-value transactions** initiated within the last 30 days for additional anomalies.
3. **Conduct a forensic examination** of Workstation-F01 for potential traces of exfiltrated data.
4. **Review and strengthen access control policies**, specifically around administrative permissions and transaction approvals
5.