Fraud detection and investigation steps

From: Vinay Sheel Pathak vinay.sheelpathak@outlook.com
To: ENSHEELVIN@GMAIL.COM ENSHEELVIN@GMAIL.COM
Sent: Thursday, 1 August at 14:10

Step-by-Step Process for Detection and Investigation of Various Types of Fraud at Barclays Bank

1. **First-Party Fraud**

Detection:
1. **Anomaly Detection**: Use machine learning algorithms to identify unusual transaction patterns that deviate from the customer's typical behavior.
2. **Behavioral Analysis**: Monitor for changes in behavior, such as sudden increases in spending, frequent high-value transactions, or unusual locations.
3. **Credit Scoring**: Regularly update and monitor customers' credit scores for unexpected changes.

Investigation:
1. **Initial Review**: Flagged transactions are reviewed by a fraud analyst to determine if further investigation is needed.
2. **Customer Contact**: Contact the customer to verify the flagged transactions.
3. **Account Monitoring**: Place the account under increased surveillance to detect further suspicious activity.
4. **Data Gathering**: Collect all relevant data, including transaction logs, communication records, and account history.
5. **Report Findings**: Document the findings and prepare a detailed report outlining the nature of the fraud and any identified perpetrators.
6. **Take Action**: Depending on the findings, take appropriate action, such as freezing the account, reversing fraudulent transactions, and collaborating with law enforcement if necessary.

2. **Account Takeover (ATO)**

Detection:
1. **Login Monitoring**: Use AI to detect unusual login patterns, such as logins from new devices or locations.
2. **Multi-Factor Authentication (MFA)**: Implement and monitor MFA to ensure only authorized users gain access.
3. **Behavioral Biometrics**: Analyze user behavior during login (e.g., typing patterns) to detect anomalies.

Investigation:
1. **Account Lockdown**: Immediately lock the compromised account to prevent further unauthorized access.
2. **Customer Notification**: Inform the affected customer about the suspected account takeover.
3. **Data Collection**: Gather data on the unauthorized access, including IP addresses, timestamps, and attempted transactions.
4. **Root Cause Analysis**: Determine how the account was compromised (e.g., phishing, malware).
5. **Remediation**: Guide the customer through securing their account, such as changing passwords and updating security questions.
6. **Report and Follow-Up**: Document the incident and follow up with the customer to ensure no further issues.

3. **ACH Fraud**

Detection:
1. **Transaction Monitoring**: Implement real-time monitoring of ACH transactions for unusual patterns or amounts.
2. **Account Reconciliation**: Regularly reconcile accounts to identify discrepancies.
3. **Alerts and Notifications**: Set up alerts for high-value transactions or transfers to new payees.

Investigation:
1. **Transaction Review**: Analyze the suspicious ACH transactions to confirm fraud.
2. **Customer Verification**: Contact the customer to verify if they authorized the transaction.
3. **Suspend Transfers**: Temporarily suspend further ACH transfers from the account until the issue is resolved.
4. **Gather Evidence**: Collect transaction records, communication logs, and any other relevant data.
5. **Collaboration**: Work with other banks and financial institutions involved in the ACH transfer to trace and recover funds.
6. **Documentation**: Prepare a detailed report of the investigation and findings.

4. **Chargeback Fraud**

Detection:
1. **Transaction Monitoring**: Monitor for patterns indicative of chargeback fraud, such as frequent chargebacks from the same customer.
2. **Order Review**: Implement additional checks for high-risk orders, such as verifying shipping addresses and

customer details.
3. **Customer History**: Review the customer's transaction history for previous chargeback instances.

Investigation:
1. **Initial Review**: Review the chargeback claim and the associated transaction details.
2. **Customer Contact**: Contact the customer to discuss the chargeback and gather their side of the story.
3. **Document Collection**: Collect all relevant documents, such as receipts, shipping information, and communication records.
4. **Analysis**: Compare the chargeback claim with the collected evidence to identify inconsistencies.
5. **Resolution**: Decide whether to accept or dispute the chargeback based on the evidence.
6. **Reporting**: Document the investigation process and the final resolution.

5. **Phishing and ID Theft**

Detection:
1. **Email Filtering**: Use advanced email filters to detect and block phishing emails.
2. **User Education**: Regularly educate customers and employees about phishing tactics and how to avoid them.
3. **Login Monitoring**: Monitor for unusual login attempts that may indicate compromised credentials.

Investigation:
1. **Immediate Action**: If phishing is detected, inform affected customers immediately to change their passwords and secure their accounts.
2. **Source Identification**: Trace the phishing attempt to its source, if possible, to block further attempts.
3. **Evidence Collection**: Gather emails, IP addresses, and other relevant data related to the phishing attempt.
4. **Collaboration**: Work with internet service providers and cybersecurity experts to shut down phishing sites.
5. **Customer Support**: Assist affected customers in securing their accounts and recovering from the attack.
6. **Documentation**: Prepare a comprehensive report on the phishing attempt and the response measures taken.

By following these structured processes, Barclays Bank can effectively detect and investigate various types of fraud, minimizing the risk and impact on customers and the bank itself.