Standard Operating Procedure: Financial Fraud Incident Response

Document Version: 1.0
Effective Date: May 19, 2025
Issuing Department: Fraud Prevention and Security Operations
Approved By: Utopia PRA

Table of Contents

1. Introduction

1.1. Purpose of this SOP

This Standard Operating Procedure (SOP) document provides a structured framework for Cymbal FinServ Ltd to effectively respond to, manage, investigate, and mitigate the impact of various types of financial fraud. Its primary goal is to ensure a consistent, timely, and compliant response to protect our customers, the organization's assets, and its reputation.

1.2. Scope

This SOP applies to all employees, contractors, and relevant third-party vendors of Cymbal FinServ Ltd who are involved in or may encounter incidents of financial fraud. This includes, but is not limited to, personnel in Customer Service, Fraud Operations, Security Operations, IT, Legal, Compliance, and Risk Management departments.

1.3. General Principles for Fraud Response

- **Timeliness:** Rapid response is critical to minimize loss and preserve evidence.
- **Confidentiality:** All fraud investigations must be handled with the utmost confidentiality.
- **Integrity:** Evidence must be collected and preserved in a forensically sound manner.
- **Customer Focus:** Affected customers must be treated with empathy and supported throughout the process.
- **Compliance:** All actions must adhere to relevant legal, regulatory, and internal policy requirements.
- **Collaboration:** Effective response requires close collaboration between various internal departments and, where appropriate, external agencies.

1.4. Roles and Responsibilities

- **Fraud Operations Team:** Primary responsibility for investigating reported fraud incidents, liaising with customers, and implementing containment measures.
- **Security Operations Team (SOC):** Responsible for technical investigation aspects, system security, log analysis, and responding to security alerts related to fraud.
- **IT Department:** Supports SOC and Fraud Operations with system access, data retrieval, and technical expertise.
- **Customer Service:** Often the first point of contact for fraud reports; responsible for initial information gathering and escalating to the Fraud Operations Team.
- **Legal & Compliance Department:** Provides guidance on legal and regulatory

obligations, assists with reporting to authorities, and manages legal actions.

- **Risk Management:** Assesses overall fraud risk exposure and contributes to the enhancement of preventative controls.

2. Section 1: Identity Theft and Synthetic Identity Fraud

2.1. Definition

Identity Theft is the fraudulent acquisition and use of an individual's personally identifiable information (PII), such as name, date of birth, address, Social Security number, or bank account details, typically for financial gain.
Synthetic Identity Fraud involves creating a fictitious identity by combining real (often stolen) PII with fabricated information. Fraudsters use these synthetic identities to open accounts, obtain credit, and commit other fraudulent acts, making them harder to detect as they don't directly map to a single, real victim initially.

2.2. Reporting Channels

- Customer reports (via phone, email, online portal, in-person).
- Internal alerts from fraud detection systems (e.g., unusual account opening patterns, mismatched PII).
- Referrals from other financial institutions or law enforcement.
- Employee vigilance and reporting.

2.3. Detailed Response Protocol

2.3.1. Initial Report Handling & Verification

Upon receiving a report of potential identity theft or synthetic identity fraud, the receiving personnel (typically Customer Service or Fraud Operations) must gather comprehensive details from the reporter. This includes the victim's full PII, a detailed account of the suspected fraudulent activity, dates, amounts involved, and any supporting documentation (e.g., unauthorized account statements, credit report discrepancies). Empathy and clear communication are crucial when dealing with victims.

The initial verification process involves cross-referencing the reported information with internal systems and databases. For synthetic identities, this may involve checking for inconsistencies in application data, unusual combinations of PII, or links to known fraudulent schemes. The authenticity of the report and the reporter's identity should be confirmed where possible.

2.3.2. Investigation & Evidence Gathering

A dedicated fraud investigator will be assigned to the case. The investigation will focus on:

- Confirming if Cymbal FinServ Ltd's accounts or services were used.
- Analyzing application data for new accounts, looking for red flags such as CPNs (Credit Privacy Numbers), unusual address history, or inconsistencies in PII.

- Reviewing transaction histories, IP logs, device information, and communication records associated with the suspected fraudulent activity.
- Identifying any other accounts or individuals potentially linked to the fraud.
- Collecting all relevant documentation, including application forms, copies of identification (if provided, and its authenticity), transaction records, and correspondence.
- Checking against internal and external fraud databases (e.g., CIFAS in the UK).

2.3.3. Containment & Impact Minimization

Immediate action is required to prevent further loss. This includes:

- Placing holds or blocks on any accounts confirmed to be fraudulent or at high risk.
- Suspending any services or credit lines associated with the compromised or synthetic identity.
- Identifying and flagging associated PII elements (addresses, phone numbers, SSNs) within internal systems to prevent their future use in fraudulent applications.
- If internal systems or data were breached to facilitate the identity theft, the SOC must be engaged to identify and remediate the vulnerability.

2.3.4. Victim Support & Communication

For victims of identity theft:

- Provide clear information on the steps taken by Cymbal FinServ Ltd.
- Advise the victim to report the identity theft to relevant credit reporting agencies (e.g., Experian, Equifax, TransUnion) and to consider placing fraud alerts or credit freezes on their files.
- Guide them on reporting the incident to law enforcement (e.g., Action Fraud in the UK, or the local police).
- Provide resources such as template letters for disputing fraudulent accounts or charges.
- Explain Cymbal FinServ Ltd's policy on liability for any losses incurred through its accounts.
  For synthetic identity fraud, direct victim impact may be less clear initially, but communication with any individual whose PII was misused is essential.

2.3.5. Regulatory Reporting & Law Enforcement Liaison

- Assess if the incident requires reporting to regulatory bodies. For example, if PII managed by Cymbal FinServ Ltd was compromised leading to identity theft, a data breach notification to the Information Commissioner's Office (ICO) in the UK

might be necessary.
- File Suspicious Activity Reports (SARs) or equivalents (e.g., to the National Crime Agency - NCA in the UK) if there is suspicion of money laundering or other serious financial crimes.
- Cooperate fully with law enforcement agencies, providing them with all relevant evidence and information gathered during the internal investigation.

2.3.6. Remediation & Recovery

- For legitimate victims, reverse any unauthorized transactions and correct account information.
- Close any fraudulently opened accounts.
- Attempt to recover any financial losses where possible, though this is often challenging with identity theft, especially synthetic ID fraud.
- Update internal systems to reflect the compromised status of PII elements.

2.3.7. Post-Incident Analysis & Prevention Enhancement

After the case is resolved, conduct a thorough review to:

- Identify how the identity theft or synthetic identity fraud occurred.
- Assess the effectiveness of existing fraud detection and prevention controls.
- Implement improvements to application screening processes, identity verification methods, and anomaly detection rules.
- Update employee training on identifying red flags associated with identity and synthetic identity fraud.

2.4. Standard Procedural Steps

1. **Log Incident:** Receive and log the report in the Incident Management System (IMS) with a unique case ID. Gather all initial details (reporter, date/time, PII involved, suspected activity, supporting documents).
2. **Initial Verification:** Verify the reporter's identity and the preliminary details of the alleged fraud. Assess severity.
3. **Alert Security Operations Team (SOC):** Create an immediate alert and escalate to the SOC and Fraud Investigation Unit. Include case ID and a summary of the suspected identity/synthetic identity fraud.
4. **Block Associated Accounts/PII:**
    - Identify and immediately block or place a high-risk flag on any accounts opened using the stolen or synthetic identity within Cymbal FinServ Ltd's systems.
    - Flag associated PII elements (addresses, phone numbers, etc.) to prevent further misuse in new applications.

   - Suspend any credit lines or services linked to these accounts.
5. **Preserve Evidence:** Secure and preserve all relevant logs, application data, transaction records, communications, and any provided identification documents.
6. **Conduct Investigation:**
   - Assign an investigator.
   - Analyze application details, PII consistency, IP addresses, device information, and transaction patterns.
   - Check internal and external fraud databases.
   - Interview the victim (if applicable) and any relevant internal staff.
7. **Victim Communication & Support:**
   - Inform the victim of actions taken by Cymbal FinServ Ltd.
   - Advise on reporting to credit bureaus, law enforcement, and placing fraud alerts.
   - Provide resources and guidance for identity recovery.
8. **Regulatory & Law Enforcement Reporting:**
   - Determine if regulatory reporting is required (e.g., ICO for data breach, SARs to NCA).
   - **If criteria are met, prepare and file the necessary reports within mandated timelines.** Document submission.
   - Report to Action Fraud or local police, providing necessary evidence.
9. **Remediate & Recover:**
   - Reverse unauthorized transactions on legitimate victim accounts if applicable.
   - Formally close fraudulent accounts.
   - Attempt recovery of losses if feasible.
10. **Post-Incident Review & Closure:**
    - Document all findings, actions, and outcomes in the IMS.
    - Conduct a post-incident review to identify control weaknesses and areas for improvement in identity verification and fraud detection.
    - Update fraud prevention strategies and training.
    - Formally close the case.

3. Section 2: Account Takeover (ATO) Fraud

3.1. Definition

Account Takeover (ATO) Fraud occurs when a malicious actor gains unauthorized access to a legitimate user's existing account (e.g., bank account, credit card, online service account). Once access is gained, the fraudster can perform unauthorized transactions, change account details, steal personal information, or use the account for other illicit purposes. ATO is often facilitated by stolen credentials (phishing, malware, data breaches), social engineering, or SIM swapping.

3.2. Reporting Channels

- Customer reports of suspicious activity on their account (unauthorized transactions, login alerts from unfamiliar devices/locations, changes to contact details).
- Internal alerts from fraud detection systems (e.g., unusual login attempts, rapid changes to account settings, high-risk transactions).
- Notifications from other institutions or law enforcement.

3.3. Detailed Response Protocol

3.3.1. Initial Report Handling & Verification

When a customer reports suspected ATO, or an internal alert is triggered, immediate attention is required. The initial handler must:

- Verify the identity of the customer reporting the issue using established multi-factor authentication protocols (being mindful that some verification methods might be compromised).
- Gather specific details: what suspicious activity was observed, when it occurred, any known or suspected cause (e.g., clicked a phishing link, lost device), and the extent of potential unauthorized access.
- Review recent account activity for immediate red flags such as logins from unusual IP addresses or geolocations, recent password or contact information changes, addition of new payees, or high-value/unusual transactions.

3.3.2. Investigation & Evidence Gathering

The assigned fraud investigator will conduct a detailed investigation, focusing on:

- **Access Vector Analysis:** Determining how the account was compromised (e.g., phishing, malware on the customer's device, credential stuffing, SIM swap, insider threat). This involves analyzing login attempt logs, IP addresses, user-agent strings, device IDs, and security alerts.

- **Scope of Compromise:** Identifying all unauthorized activities performed by the fraudster, including transactions, data viewed or exfiltrated, changes made to account settings, and any linked accounts that might also be at risk.
- **Timeline Reconstruction:** Establishing a clear timeline of the fraudulent activity from initial unauthorized access to detection.
- **Evidence Preservation:** Collecting and preserving all relevant digital evidence, such as server logs, transaction records, security event logs, and customer communications.

3.3.3. Containment & Impact Minimization

Rapid containment is crucial:

- Immediately suspend or lock the compromised account to prevent further unauthorized access and transactions.
- Invalidate current login credentials and session tokens.
- Review and revert any unauthorized changes made to the account (e.g., email address, phone number, shipping address, password).
- Block any identified malicious IP addresses or devices at the network/application level.
- If malware is suspected on the customer's device, advise the customer on steps to scan and clean their devices.
- If a SIM swap is suspected, advise the customer to contact their mobile carrier immediately.

3.3.4. Victim Support & Communication

- Keep the legitimate account holder informed throughout the investigation process.
- Explain the security measures taken to protect their account.
- Guide the customer through the process of securely regaining access to their account, which typically involves resetting passwords and re-establishing multi-factor authentication (MFA).
- Advise the customer on best practices for account security (e.g., strong unique passwords, MFA, recognizing phishing attempts).
- Discuss Cymbal FinServ Ltd's policy on liability for unauthorized transactions resulting from ATO.

3.3.5. Regulatory Reporting & Law Enforcement Liaison

- Assess if the ATO incident constitutes a data breach (e.g., if sensitive PII was accessed or exfiltrated) requiring notification to regulatory bodies like the ICO.
- File SARs if the unauthorized transactions suggest money laundering or other

reportable offenses.

- Cooperate with law enforcement if they become involved, providing necessary evidence and information.

3.3.6. Remediation & Recovery

- Reverse any confirmed unauthorized transactions according to Cymbal FinServ Ltd's policy and relevant regulations (e.g., payment services regulations).
- Assist the customer in restoring their account to its pre-incident state.
- Work with the customer to identify and dispute any further fraudulent activity that may have occurred as a result of the ATO (e.g., on linked external accounts if information was stolen).
- Attempt to recover funds transferred fraudulently, although this can be difficult, especially if funds were moved quickly through multiple accounts or converted to cryptocurrency.

3.3.7. Post-Incident Analysis & Prevention Enhancement

- Analyze the root cause of the ATO (e.g., weak customer passwords, successful phishing campaign, vulnerability in authentication mechanisms).
- Evaluate the effectiveness of existing ATO detection and prevention controls (e.g., MFA, behavioral biometrics, transaction monitoring rules).
- Implement enhancements, such as stronger authentication requirements, improved user alerts for suspicious activity, and more sophisticated anomaly detection.
- Update customer education materials on ATO prevention.
- Review and update internal training for fraud and customer service teams.

3.4. Standard Procedural Steps

1. **Log Incident:** Receive and log the ATO report/alert in the IMS with a unique case ID. Gather details of suspicious activity, customer information, and potential compromise vector.
2. **Verify Customer & Initial Assessment:** Securely verify the identity of the reporting customer. Perform an initial assessment of account activity for immediate red flags.
3. **Alert Security Operations Team (SOC):** Create an immediate alert and escalate to the SOC and Fraud Investigation Unit. Include case ID, account details, and summary of suspected ATO.
4. **Block Access to Associated Accounts:**
   - Immediately suspend or lock the compromised customer account(s).
   - Invalidate current login credentials and active sessions.
   - Prevent any further transactions or changes to account details until control is

re-established.

5. **Preserve Evidence:** Secure and preserve all relevant logs (login, transaction, security event), IP addresses, device IDs, and customer communications.
6. **Conduct Investigation:**
    - Assign an investigator.
    - Determine the access vector (phishing, malware, credential stuffing, etc.).
    - Identify the full scope of unauthorized activities and data exposure.
    - Reconstruct the timeline of the ATO incident.
7. **Victim Communication & Support:**
    - Maintain regular communication with the affected customer.
    - Guide them through securing their account (password reset, MFA setup).
    - Advise on protecting their devices and other online accounts.
8. **Regulatory & Law Enforcement Reporting:**
    - Determine if the incident requires reporting as a data breach (e.g., to ICO) or for other regulatory purposes (e.g., SARs to NCA).
    - **If criteria are met, prepare and file the necessary reports within mandated timelines.** Document submission.
    - Report to Action Fraud or local police if appropriate.
9. **Remediate & Recover:**
    - Reverse confirmed unauthorized transactions as per policy.
    - Assist the customer in restoring their account securely.
    - Attempt recovery of lost funds where feasible.
10. **Post-Incident Review & Closure:**
    - Document all findings, actions, and outcomes in the IMS.
    - Conduct a post-incident review to identify root causes and improve ATO prevention/detection controls (e.g., authentication methods, user alerts).
    - Update customer education and internal training.
    - Formally close the case.

4. Section 3: Authorized Push Payment (APP) Fraud & Social Engineering Scams

4.1. Definition

Authorized Push Payment (APP) Fraud occurs when a fraudster deceives an individual or a business into willingly sending money (making a "push payment") from their account to an account controlled by the fraudster. This is achieved through various social engineering tactics, where the victim believes they are making a legitimate payment. Examples include impersonation scams (e.g., pretending to be from a bank, HMRC, or a supplier), investment scams, and romance scams.

4.2. Reporting Channels

- Customer reports that they have been tricked into making a payment to a fraudster.
- Internal alerts if fraud detection systems identify suspicious outgoing payments or known mule accounts.
- Information from other banks (e.g., via a fraud reporting scheme) indicating a payment from a Cymbal FinServ Ltd customer may be fraudulent.

4.3. Detailed Response Protocol

4.3.1. Initial Report Handling & Verification

When a customer reports a suspected APP fraud:

- Treat the customer with empathy, as they are often distressed and may feel embarrassed.
- Gather detailed information about the scam: how the customer was contacted, the nature of the deception, the information provided to the fraudster, details of the payment(s) made (amount, date, recipient account details), and any ongoing contact with the fraudster.
- Verify the customer's identity and the details of the reported transactions from internal systems.
- Act with extreme urgency, as the speed of response is critical for any chance of fund recovery.

4.3.2. Investigation & Evidence Gathering

The investigation will focus on:

- **Understanding the Scam:** Analyzing the fraudster's methodology, including the communication channels used (email, phone, social media), the impersonation tactics, and the specific instructions given to the victim.

- **Tracing Payments:** Identifying the beneficiary account details and the receiving bank.
- **Evidence Collection:** Gathering all relevant evidence, including customer statements, transaction records, copies of communications with the fraudster (emails, messages), and any details the customer can provide about the fraudster's persona or contact information.
- **Mule Account Identification:** Determining if the recipient account is a known mule account or exhibits characteristics of one.

4.3.3. Containment & Impact Minimization

- **Immediate Fund Recovery Attempts:** If the report is received quickly after the payment, immediately contact the receiving bank to request that the funds be frozen and returned (e.g., using industry schemes like the UK's CRM - Contingent Reimbursement Model - protocols, or payment recall mechanisms).
- Advise the customer to cease all contact with the suspected fraudster.
- If the customer's online banking credentials or other sensitive information were compromised during the scam, take steps to secure their Cymbal FinServ Ltd accounts (as per ATO procedures).
- Flag the beneficiary account details in internal systems and share with industry databases if appropriate.

4.3.4. Victim Support & Communication

- Provide ongoing updates to the customer about the status of the investigation and any fund recovery efforts.
- Explain Cymbal FinServ Ltd's policy on APP fraud, including any potential for reimbursement (e.g., under the CRM code if applicable, or other discretionary policies). This is a sensitive area and requires clear, careful communication.
- Offer advice on how to avoid future scams and where to find further support (e.g., victim support organizations).
- Acknowledge the emotional impact of APP fraud and direct them to resources if needed.

4.3.5. Regulatory Reporting & Law Enforcement Liaison

- File SARs for all APP fraud cases, as they involve the movement of illicit funds.
- Report the incident to Action Fraud or the relevant national fraud reporting center.
- Cooperate with the receiving bank in their investigation and any efforts by law enforcement to trace and prosecute the fraudsters.
- Comply with any specific regulatory requirements related to APP fraud reporting

or reimbursement schemes.

4.3.6. Remediation & Recovery

- Process any reimbursement to the victim in line with Cymbal FinServ Ltd's policy and regulatory obligations. This is a key area of focus for APP fraud.
- If funds are successfully recovered from the receiving bank, ensure they are returned to the victim promptly.
- Document all recovery attempts, successes, and failures. Recovery rates for APP fraud are often low due to the speed at which fraudsters move funds.

4.3.7. Post-Incident Analysis & Prevention Enhancement

- Analyze the APP fraud incident to understand the specific social engineering tactics used.
- Review the effectiveness of warnings and customer education provided by Cymbal FinServ Ltd.
- Enhance transaction monitoring rules to detect patterns indicative of APP fraud (e.g., payments to new beneficiaries with high-risk characteristics).
- Improve customer awareness campaigns about common APP scams and how to recognize them (e.g., "confirmation of payee" warnings, being wary of urgent requests).
- Share anonymized intelligence with industry bodies to help combat APP fraud more broadly.

4.4. Standard Procedural Steps

1. **Log Incident:** Receive and log the APP fraud report in the IMS with a unique case ID. Gather details of the scam, communication methods, payment details (amount, date, recipient account/bank).
2. **Verify Customer & Initial Assessment:** Verify the customer's identity. Assess the urgency, focusing on the time elapsed since the payment.
3. **Alert Security Operations Team (SOC) & Fraud Team:** Create an immediate alert and escalate to the Fraud Investigation Unit and SOC (if any technical compromise is also suspected).
4. **Attempt Immediate Fund Recovery (Block Access to Funds by Fraudster):**
   - **Immediately contact the receiving bank** to request the freezing and return of funds. Provide all relevant transaction details.
   - If the customer's own accounts or credentials were compromised during the scam, block access to those accounts as per ATO procedures.
5. **Preserve Evidence:** Collect customer statements, transaction records, communications with the fraudster, and recipient account details.
6. **Conduct Investigation:**

   - Assign an investigator.
   - Analyze the scam methodology and social engineering tactics.
   - Trace payment flows and identify recipient bank/account.
   - Interview the victim for a full account of events.

7. **Victim Communication & Support:**
   - Keep the victim informed of recovery efforts and investigation progress.
   - Explain Cymbal FinServ Ltd's APP fraud policy and potential for reimbursement.
   - Advise the victim to cease contact with fraudsters and report to relevant bodies.
   - Offer support resources.
8. **Regulatory & Law Enforcement Reporting:**
   - **File a SAR with the NCA (or equivalent) for all APP fraud cases.**
   - Report the incident to Action Fraud (or national equivalent).
   - Cooperate with receiving banks and law enforcement.
9. **Remediate & Recover:**
   - Process any eligible reimbursement to the victim according to policy and regulatory schemes (e.g., CRM).
   - Return any recovered funds to the victim.
10. **Post-Incident Review & Closure:**
    - Document all findings, actions, recovery attempts, and outcomes in the IMS.
    - Conduct a post-incident review to identify trends in APP scams and improve customer warnings, education, and detection systems.
    - Update fraud prevention strategies.
    - Formally close the case.

5. Section 4: Business Email Compromise (BEC) Fraud

5.1. Definition

Business Email Compromise (BEC) Fraud is a sophisticated scam targeting businesses (and sometimes individuals) where fraudsters impersonate company executives (e.g., CEO, CFO), employees, or trusted third-party vendors via email or other electronic communication. The goal is to trick an employee with financial authority into making unauthorized wire transfers, changing payment details for legitimate invoices to fraudster-controlled accounts, or divulging sensitive company information.

5.2. Reporting Channels

- Internal reports from employees who have received suspicious emails or payment requests.
- Finance department identifying unusual payment requests or discrepancies.
- Alerts from IT/Security regarding compromised email accounts.
- Notifications from vendors or partners whose email accounts may have been compromised and used to target Cymbal FinServ Ltd.
- Discovery of unauthorized transactions.

5.3. Detailed Response Protocol

5.3.1. Initial Report Handling & Verification

When a potential BEC incident is reported:

- **Treat as highly urgent.** The speed of response is critical to prevent or recover financial loss.
- The initial recipient (e.g., employee's manager, IT helpdesk, Fraud team) must immediately escalate to the designated BEC Incident Response team (often a combination of Fraud, IT/Security, and Finance).
- Verify the authenticity of the report. If an employee received a suspicious email, they should not reply or click links but forward it as an attachment to IT/Security for analysis.
- If a payment has already been made, gather all details: amount, beneficiary account, receiving bank, date, and any related communications.

5.3.2. Investigation & Evidence Gathering

The investigation involves multiple facets:

- **Email Analysis (IT/Security):** Examine the suspicious email(s) for signs of spoofing, phishing, or account compromise (e.g., review email headers, sender's actual address, embedded links, malware). Determine if an internal email account was compromised or if it's an external impersonation.

- **Payment Tracing (Fraud/Finance):** If a payment was made, immediately trace the funds.
- **Internal Process Review:** Understand how the fraudulent request bypassed internal controls. Interview the employee(s) involved to understand the sequence of events and the nature of the deception.
- **Scope Assessment:** Determine if other employees received similar requests or if other systems/data were compromised.
- **Evidence Collection:** Preserve all relevant emails, transaction records, internal communication logs, and system logs.

5.3.3. Containment & Impact Minimization

- **Stop/Recall Payments:** If a fraudulent payment has been made, immediately contact Cymbal FinServ Ltd's bank to request a payment recall or reversal. Contact the beneficiary bank to alert them to the fraud and request the funds be frozen.
- **Secure Compromised Accounts:** If an internal email account is found to be compromised, immediately reset the password, revoke active sessions, enable/verify MFA, and scan the user's devices for malware. IT/Security will conduct a broader assessment for other compromised accounts.
- **Internal Alert:** Issue an internal alert to relevant employees (especially in finance and payment processing roles) about the ongoing BEC attempt, detailing the tactics used and advising vigilance.
- **Block Malicious Indicators:** Block sender email addresses, domains, or IPs identified as malicious.

5.3.4. Victim Support & Communication (Internal & External)

- **Internal Communication:** Keep relevant internal stakeholders (management, legal, finance, IT, security) informed of the incident status, impact, and remediation efforts. Support employees who were targeted or tricked, emphasizing that BEC scams are sophisticated and designed to deceive.
- **External Communication (if applicable):** If the BEC involved impersonating a vendor, or if a vendor's email was compromised to target Cymbal FinServ Ltd, communication with that vendor is necessary. If Cymbal FinServ Ltd's email was compromised to target others, those parties may need to be notified.

5.3.5. Regulatory Reporting & Law Enforcement Liaison

- File SARs if the BEC incident involves significant financial loss or suspicious transactions.

- Report the incident to national fraud reporting centers (e.g., Action Fraud in the UK, IC3 in the US).
- Cooperate fully with law enforcement investigations.
- If the BEC incident involved a data breach (e.g., unauthorized access to sensitive information within a compromised email account), assess if notification to regulatory bodies like the ICO is required.

5.3.6. Remediation & Recovery

- Work with banks to recover any fraudulently transferred funds. Success rates vary and depend on the speed of action.
- Review and strengthen internal payment authorization processes (e.g., implement mandatory out-of-band verification for changes to vendor payment details or urgent/unusual payment requests).
- Address any vulnerabilities identified in email security or internal controls.

5.3.7. Post-Incident Analysis & Prevention Enhancement

- Conduct a detailed post-mortem of the BEC incident to understand the root cause and control failures.
- Enhance employee training on recognizing BEC red flags (e.g., sense of urgency, requests for secrecy, slight variations in email addresses, unusual language or requests from known contacts).
- Implement or improve technical controls such as advanced email filtering, DMARC/DKIM/SPF records, and endpoint security.
- Regularly test internal processes through simulated BEC attacks.
- Update vendor management processes to include secure methods for verifying changes to payment information.

5.4. Standard Procedural Steps

1. **Log Incident:** Receive and log the BEC report/alert in the IMS with a unique case ID. Gather details of the suspicious communication, requested action (e.g., payment), and any payments already made.
2. **Immediate Escalation & Verification:** Escalate immediately to the BEC Incident Response team (Fraud, IT/Security, Finance). Verify the nature of the threat (e.g., compromised internal account vs. external spoofing).
3. **Alert Security Operations Team (SOC) & Relevant Departments:** Create an immediate alert for the SOC for technical investigation (email analysis, account compromise). Alert Finance and payment teams.
4. **Attempt Payment Recall / Block Access:**
    - **If a payment was made, immediately contact Cymbal FinServ Ltd's bank to initiate a payment recall and alert the beneficiary bank.**

  - If an internal email account is suspected to be compromised, **IT/Security must immediately block access to the account**, reset credentials, revoke sessions, and investigate further.
5. **Preserve Evidence:** Secure and preserve all suspicious emails (including full headers), transaction records, communication logs, and system logs.
6. **Conduct Investigation:**
   - IT/Security: Analyze email for authenticity, malware, and compromise vector. Check for wider compromise.
   - Fraud/Finance: Investigate payment details, internal processes bypassed, and interview involved staff.
7. **Internal Communication & Alert:**
   - Issue an internal alert to relevant staff about the BEC attempt, detailing tactics.
   - Support affected employees.
8. **Regulatory & Law Enforcement Reporting:**
   - **File a SAR with the NCA (or equivalent) if financial loss or suspicion of money laundering occurs.**
   - Report to Action Fraud (or national equivalent) and cooperate with law enforcement.
   - Assess data breach reporting obligations (e.g., to ICO) if sensitive data was exposed.
9. **Remediate & Recover:**
   - Pursue fund recovery vigorously.
   - Implement out-of-band verification for payment changes.
   - Address technical and procedural vulnerabilities.
10. **Post-Incident Review & Closure:**
    - Document all findings, actions, and outcomes in the IMS.
    - Conduct a thorough post-mortem. Enhance BEC awareness training, email security controls, and payment authorization procedures.
    - Formally close the case.

6. Section 5: Payment Card Fraud (Debit/Credit Card Fraud)

6.1. Definition

Payment Card Fraud is the unauthorized use of a debit or credit card, or its details, to make purchases, withdraw cash, or conduct other transactions without the account holder's permission. This can occur through various means, including lost or stolen cards, card-not-present (CNP) fraud (using stolen card details online or over the phone), skimming (capturing card data at ATMs or POS terminals), or account takeover leading to card misuse.

6.2. Reporting Channels

- Customer reports of unauthorized transactions on their card statements.
- Alerts from Cymbal FinServ Ltd's card fraud detection systems (e.g., based on unusual transaction patterns, high-risk merchant categories, geographic anomalies).
- Notifications from card networks (Visa, Mastercard, etc.) about potentially compromised cards (e.g., through a merchant data breach).
- Reports of lost or stolen cards by customers.

6.3. Detailed Response Protocol

6.3.1. Initial Report Handling & Verification

When a customer reports suspected card fraud or an alert is generated:

- Verify the customer's identity using secure authentication methods.
- Gather details of the disputed transaction(s): merchant name, date, amount, location.
- If the card is reported lost or stolen, confirm the last known legitimate use.
- Review recent transaction history for other suspicious activities.

6.3.2. Investigation & Evidence Gathering

The investigation by the Card Fraud team will involve:

- **Transaction Analysis:** Examining the details of the disputed transactions, including merchant category codes (MCCs), transaction types (e.g., card-present, CNP, ATM withdrawal), IP addresses for online transactions, and shipping addresses if applicable.
- **Common Point of Purchase (CPP) Analysis:** If multiple customers report fraud after using their cards at the same merchant, this may indicate a data breach at that merchant or a skimming operation.
- **Skimming/Shimming Detection:** Reviewing alerts or reports related to

compromised ATMs or POS devices.

- **Card Usage Patterns:** Comparing fraudulent transactions to the customer's legitimate spending habits.
- **Evidence Collection:** Gathering transaction records, merchant details, customer statements, and any information from card networks or fraud detection systems.

6.3.3. Containment & Impact Minimization

- **Block the Card:** Immediately block the compromised debit or credit card to prevent further unauthorized transactions.
- **Issue a New Card:** Arrange for a replacement card to be issued to the customer with a new card number.
- **Review Linked Services:** Check if the compromised card was used for recurring payments or linked to digital wallets, and advise the customer accordingly.
- If a merchant breach is suspected as the CPP, this information should be escalated for potential broader action or notification via card schemes.

6.3.4. Victim Support & Communication

- Inform the customer that their card has been blocked and a new one is being issued.
- Explain the dispute process for the unauthorized transactions.
- Provide guidance on reviewing future statements carefully.
- Advise on card security best practices (e.g., protecting PINs, being cautious with online transactions, monitoring accounts regularly).
- Clarify Cymbal FinServ Ltd's liability policy for card fraud (often, customers have zero or limited liability for unauthorized card transactions if reported promptly).

6.3.5. Regulatory Reporting & Law Enforcement Liaison

- While individual card fraud transactions may not always require a SAR unless they are part of a larger pattern of suspicious activity or money laundering, aggregate data on card fraud is often reported to regulators or industry bodies.
- Report significant fraud cases, organized skimming operations, or large-scale breaches to law enforcement and relevant card network security teams.
- Comply with Payment Card Industry Data Security Standard (PCI DSS) requirements, especially if Cymbal FinServ Ltd's systems were involved in a compromise leading to card fraud.

6.3.6. Remediation & Recovery

- Process chargebacks for confirmed fraudulent transactions according to card network rules. This involves disputing the transaction with the merchant's acquiring bank.

- Credit the customer's account for the value of the unauthorized transactions once the fraud is confirmed and the dispute is successful (or as per provisional credit policies).
- Monitor for further linked fraudulent activity.

6.3.7. Post-Incident Analysis & Prevention Enhancement

- Analyze trends in card fraud (e.g., types of merchants targeted, methods used by fraudsters).
- Review and update the rules in card fraud detection systems (e.g., FICO Falcon, or proprietary systems).
- Enhance security features for cards (e.g., EMV chip technology, tokenization, 3D Secure for CNP transactions).
- Improve customer education on card security and identifying fraudulent transactions.
- Share intelligence with card networks and other financial institutions to combat organized card fraud.

6.4. Standard Procedural Steps

1. **Log Incident:** Receive and log the card fraud report/alert in the IMS with a unique case ID. Gather customer and card details, and specifics of disputed transactions.
2. **Verify Customer & Initial Assessment:** Securely verify the customer's identity. Review recent transaction history for suspicious patterns.
3. **Alert Card Fraud Team & SOC (if applicable):** Escalate to the dedicated Card Fraud Investigation Unit. Alert SOC if a wider system compromise related to card data is suspected.
4. **Block Access (Block the Card):**
   - **Immediately block the reported compromised/lost/stolen credit or debit card.**
   - Prevent any further authorizations on that card number.
5. **Preserve Evidence:** Secure transaction records, merchant information, fraud alerts, and customer communications.
6. **Conduct Investigation:**
   - Assign an investigator.
   - Analyze disputed transactions, comparing them to legitimate spending patterns.
   - Perform CPP analysis if multiple reports emerge.
   - Investigate potential skimming or CNP fraud vectors.
7. **Victim Communication & Support:**

   - Inform the customer about the card block and reissuance of a new card.
   - Explain the dispute/chargeback process.
   - Advise on card security measures.
8. **Regulatory & Law Enforcement Reporting:**
   - File SARs if transactions are linked to broader suspicious activity or money laundering.
   - Report significant incidents or organized crime to law enforcement and card networks.
   - Adhere to PCI DSS reporting requirements if applicable.
9. **Remediate & Recover:**
   - Initiate chargeback procedures for confirmed fraudulent transactions through card network channels.
   - Credit the customer's account as per policy and successful disputes.
   - Issue a replacement card.
10. **Post-Incident Review & Closure:**
   - Document all findings, actions, and outcomes in the IMS.
   - Analyze card fraud trends to update detection rules, card security features (e.g., velocity limits, geographic blocking), and customer education.
   - Formally close the case.

7. SOP Review and Maintenance

This SOP will be reviewed and updated at least annually, or as needed in response to significant changes in the fraud landscape, regulatory requirements, internal processes, or lessons learned from fraud incidents. The [Issuing Department - e.g., Head of Fraud Prevention] is responsible for maintaining this document. All changes must be documented and approved.

8. Appendix (Placeholder)

8.1. Contact List

- Internal Teams (Fraud Operations, SOC, IT, Legal, Compliance, Customer Service Management)
- Key Regulatory Bodies (e.g., FCA, ICO, NCA)
- Law Enforcement (e.g., Action Fraud, Local Police Economic Crime Units)
- Card Networks (Visa, Mastercard Security Contacts)
- Credit Reference Agencies

8.2. Reporting Templates

- Internal Incident Report Form
- SAR Submission Checklist
- Data Breach Notification Checklist (if applicable)