**Procedure 4125.10: Corporate Account Takeover**

**Model Revised Date: 6/12/2025**

**ACCOUNT OPENING PROCEDURES/CONSIDERATIONS**

The Credit Union will consider the following procedures and considerations when opening and reviewing business member accounts (“corporate accounts”).

1. At account opening, a risk rating will be assigned to corporate accounts performing online transactions (typically done as part of initial member due diligence but can be fluid and may also be done after account opening in conjunction with the BSA Officer). Factors to be considered when assigning a risk rating include:  
   1. Type of business:  
      1. Domestic vs. International; and
      2. Retail versus wholesale;
   2. Average account balances (loans and deposits);
   3. Services utilized:  
      1. Wire transfer
      2. ACH debt origination files;
      3. ACH credit origination files; and
      4. Bill payment;
   4. Standard Entry Class (SEC) codes assigned to member’s transactions;
   5. Volume of transactions;
   6. File limits/frequency (NACHA);
   7. Security measures the business account members utilize; and
   8. Business member’s administrative controls over their users and system configurations.
2. Establish controls at the Credit Union, such as limits, to mitigate the risk of corporate accounts being taken over.  
   1. Enable “out-of-band” confirmation of payment initiation, or for certain defined types of payments; and
   2. Provide out-of-band alerts for unusual activity (red flag reports).
3. Communicate with Business Members to drive awareness as outlined in procedures.  
   1. Implement deeper training/awareness for business members who are high risk.
   2. Provide examples of potential warning signs of potentially compromised computer systems.
4. Review member agreements to ensure accountability.
5. Keep in close contact with third-party vendors to ensure security is a priority to reduce risk.  
   1. Part of the annual vendor reviews will include identification of controls in place at the third-party vendor to reduce account takeover risks.

**BUSINESS MEMBER BEST PRACTICES**

The majority of cyber thefts begin with thieves compromising the computer(s) of business members. Therefore, the Credit Union can assist the business member in providing guidance and requirements on security practices. The Credit Union will communicate some or all of the following security business practices that can be implemented to reduce risks.

1. Provide enhanced security awareness training and continuous communication to employees using online banking systems to help ensure an understanding of the security risks associated with their duties;
2. Update anti-virus and anti-malware programs frequently;
3. Update on a regular basis, all computer software to protect against new security vulnerabilities (patch management);
4. Communicate the importance of password strength and not storing passwords in easily accessible places.  
   1. Incorporate multi-factor and multi-channel authentication for corporate accounts that are permitted to initiate funds transfers. Examples:  
      1. Something the person knows (user ID, PIN, password);
      2. Something the person has (password-generated token, USB token);
5. Require business members to initiate payments under dual control, with a distinct responsibility for transaction origination and authorization;  
   1. One person authorizes the creation of the payment file;
   2. Second person authorizes the release of the file;
6. Restrict activities on computer workstations and laptops that are used for online banking and payments;  
   1. Workstations used for online banking should not be used for general web browsing and social networking; or
   2. Conduct online banking and payments activity from a dedicated computer that is not used for other online activity and not connected to an internal network;
7. Ongoing account monitoring and reconciliation, especially near the end of the day; and
8. Adopt advanced security measures by working with consultants or dedicated IT staff.

**RESPONSE PROCEDURES**

1. Immediately verify if a suspicious transaction is fraudulent;
2. Immediately attempt to reverse all suspected fraudulent transactions;  
   1. Send a “Fraudulent File Alert” through FedLine; and
   2. Immediately notify the receiving bank of the fraudulent transactions and ask them to hold or return funds;
3. Implement a plan to recover or suspend any systems suspected of being compromised. This includes conducting a forensic analysis and potentially suspending the business members’ funds transfer capabilities until results are known;
4. Immediately contact law enforcement and regulatory agencies once the initial recovery efforts have concluded; and
5. Notify the Bank Secrecy Act (BSA) Officer for a SAR filing.

**CREDIT UNION CONTROLS AND RISK MITIGATION**

The Credit Union will utilize multiple controls to help mitigate the risk associated with corporate account takeover (CATO).

1. Provide training to the Board of Directors on CATO issues and scenarios;
2. Work with the BSA Officer and the Information Security Team to detect anomalies and respond to suspicious activity related to:  
   1. Initial login and authentication for access to online banking; and
   2. Initiation of transactions to transfer funds to other parties;
3. Utilize enhanced controls over account administration, which may include:  
   1. Requiring an additional authentication prior to implementing the change;
   2. Requiring verification/confirmation of changes prior to implementing them;
   3. Providing automatic member notification (such as a text message or automated call to cell phone) immediately after implementing an administrative change;
   4. Preventing account holders from creating administrative users without Credit Union approval; and
   5. Eliminating all self-administration if the business member doesn’t meet minimum security standards established by the Credit Union;
4. Provide screen display or something similar that shows business members the number of failed logins since their prior successful login and the date and time of their last login;
5. Work with the BSA officer to ensure adequate fraud detection and monitoring systems are in place;
6. Dual business member authorization through different access devices;
7. Out-of-band verification of transactions (to/from a different device);
8. Techniques to restrict transactions such as debit blocks and debit filters;
9. Restrictions on account activity such as reasonable limits (based on historical activity) on transaction values, daily limits, who may receive funds, and time of day (and day of week) that high risk transactions such as wires and ACH originations may be initiated;
10. Tools that block connection from IP address known or suspected to be associated with fraudulent activities;
11. Policies to address potentially compromised computer equipment;
12. Enhanced controls over account maintenance activities such as changes to postal and email addresses, phone numbers, and passwords, regardless if they are performed online, by mail or by phone;
13. Use of USB devices that are read only and which function independently of the business member’s computer operating system, ensuring a secure connection to the credit union’s network;
14. Enhanced challenge questions for business member login;
15. Maintain an effective firewall and process to evaluate, monitor, and validate firewall settings on an appropriate schedule;
16. Utilize an effective patch management program that assesses patch effectiveness and implementation at least monthly; and
17. Additional security measures for employee’s computers used internally to access or manage the cash management system should include controls recommended for business members.

**MEMBER AGREEMENTS**

The Credit Union will have their business membership account agreement reviewed by legal counsel. Some critical components may include the following:

1. Roles and responsibilities for processing transaction requests and dispute resolution;
2. Minimum security standards that the Credit Union requires the business member to utilize;
3. Disclaimer and acknowledgment that no list of security practices can be all inclusive and foolproof for preventing theft;
4. Establishment of exposure limits through transaction limits, transaction frequencies, and types of payments that can be processed during the member’s normal course of business. In addition, the agreement should outline:  
   1. Process for changing limits;
   2. Provision authorizing the Credit Union to not honor a transaction request if the Credit Union in it’s sole discretion believes not processing it will protect the account holder from fraud; and
   3. Making an annual disclosure of the account agreement terms, mentioning any changes, and including a pamphlet on security awareness;
5. Disclaimer that the risk of loss resides with the account holder if a fraudulent payment order is received and the credit union processes the transaction in accordance with its normal security procedures;
6. Requirement that the business member provide a list of the employees that are authorized to initiate files, or if the business member is controlling account administration and accessibility, then an acknowledgment from the business member of their responsibility and liability; and
7. Provisions for settling contract disputes. Consideration should be given to requiring arbitration to settle contract disputes, or to include a provision that provides the account holder with warranties or indemnification against CATO thefts, providing the account holder has followed specific practices.

**MEMBER AWARENESS PROGRAM IDEAS**

Member awareness initiatives are a critical risk mitigant for the Credit Union. The following topics and training initiatives will be pursued:

1. Explanation of how business members can determine the legitimacy of communications from the credit union, particularly communications that seek information that could be used to access the business member’s account.
2. Explanation of controls the credit union offers that business members can use to mitigate risk, such as multi-factor authentication.
3. Explanation of communication mechanisms that business members may use to monitor account activity, such as transaction alerts.
4. Credit union contacts that business members can use to report suspicious account activity or information security-related events.
5. Educational information on external threats and methods used by perpetrators to illegally access accounts and account information, such as phishing, social engineering, mobile-based trojans, and business email compromise.
6. Situations where the credit union uses enhanced authentication controls, such as call center contact or certain types of account activity like password reset.
7. Explanation of the legal and other rights and protections a member may have in the event of unauthorized access to an account.

**RESOURCES**

* [Best Practices for Banks – Reducing Risk of Corporate Account Takeovers](https://www.csbs.org/sites/default/files/2017-11/BestPracticesCATO.pdf)
* [NACHA – Account Takeover](https://www.nacha.org/content/account-takeover)
* [FFIEC – Authentication and Access to Financial Institution Services and Systems](https://www.ffiec.gov/guidance/Authentication-and-Access-to-Financial-Institution-Services-and-Systems.pdf)