



# California Department of Financial Institutions

## *Best Practices Reducing the Risks of Corporate Account Takeovers*

---

### **INTRODUCTION**

A state led cooperative effort, including the United States Secret Service, developed a list of nineteen recommended processes and controls for reducing the risks of Corporate Account Takeovers. These processes and controls expand upon a three-part risk management framework developed by the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3), and the Financial Services-Information Sharing and Analysis Center (FS-ISAC)<sup>1</sup>. Fundamentally, an institution should develop risk management processes and controls centered on these three core elements:

- **Protect**
- **Detect**
- **Respond**

The following best practices have been compiled for each of the recommended processes and controls under the Protect, Detect, and Respond framework. These best practices are not an all-inclusive list and are provided as guidance to assist in implementing the nineteen processes and controls needed to reduce the risk of Corporate Account Takeover thefts. The Federal Financial Institutions Examination Council's (FFIEC) *Supplement to Authentication in an Internet Banking Environment*<sup>2</sup> (FFIEC Supplemental Guidance) issued on June 28, 2011, conveys minimum expectations which are noted within this document. It is important to remember that electronic crimes are dynamic as cyber-criminals continually change their techniques. Additional changes in risk management processes and controls will be necessary as this type of theft continues to evolve.

---

<sup>1</sup> Refer to the jointly issued "Fraud Advisory for Businesses: Corporate Account Takeover" available on the IC3 and FS-ISAC websites (<http://www.ic3.gov/media/2010/corporateaccounttakeover.pdf>) or the FS-ISAC website (<http://www.fsisac.com/files/public/db/p265.pdf>).

<sup>2</sup> The FFIEC Guidance is available at [http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20\(FFIEC%20Formatted\).pdf](http://www.ffiec.gov/pdf/Auth-ITS-Final%206-22-11%20(FFIEC%20Formatted).pdf).

## **I. Protect**

### **P1. Expand the risk assessment to incorporate Corporate Account Takeover.**

The risk assessment should include risks of Corporate Account Takeovers and be reviewed and updated at least annually for threats and risks related to online payment services. After the risk assessment is updated, an analysis should be made to identify the institution's existing controls that need to be updated or controls that need to be implemented to achieve compliance with regulatory guidance. A sample Corporate Account Takeover risk assessment is available electronically on the California Department of Financial Institutions' website, [www.dfi.ca.gov/resources](http://www.dfi.ca.gov/resources).

An effective risk management assessment should:

1. Define the scope and complexity of the institution's payment and online banking services, noting any changes since the prior risk assessment;
2. Identify what functionality is offered or has changed regarding:
  - a. Online wire transfers;
  - b. Online ACH origination;
  - c. Online bill payments; and
  - d. Delivery channels (such as mobile banking or remote deposit capture);
3. Assess if transaction limits have been set within the automated system and if those limits are appropriate;
4. Present a clear understanding of the institution's:
  - a. Customer segmentation (e.g., number of business customers or types of customers adopting online banking) and any changes that have occurred;
  - b. Customer utilization of online banking services - type and extent; and
  - c. Expected electronic payment volumes (size and frequency of wires and ACH origination files – both the average and peak volumes);
5. Assess reliance on third-party service providers for electronic payment processing and deliver of online banking services<sup>3</sup>;
6. Determine and assess on-going customer education and training practices;
7. Identify and assess all "automated pass-through" payment processing activities (e.g. online, real-time instructions for wire/ACH transactions that are automatically passed to the payment system operator, usually the Federal Reserve Bank (FRB) or a Corporate Credit Union, for processing or that are automatically passed to a bill payment system) and assess practices for reviewing automated anomaly detection alerts;
8. Identify and assess manual controls (and/or any automated anomaly detection) used to evaluate transactions that are not automatically sent to processor;
9. Determine the ability of corporate customers to correct, update, or change ("uninitiate") a transaction without further confirmation/authentication of the final transaction's instruction;
10. Assess the training and awareness of institution employees that process incoming transfer instructions, as well as the adequacy of staffing for these activities;
11. Assess the competency of the institution's staff responsible for sustaining adequate risk management practices related to ever evolving electronic payment risks, which includes considering available resources such as service providers and security and audit vendors;
12. Identify the most significant types of fraud being experienced by the industry and the emerging threats;
13. Evaluate the degree to which IT security training is provided to all institution employees including managers and front line customer contact employees. (Is there a strong corporate culture of security?); and
14. Assess the need for electronic theft insurance. If this type of insurance has been purchased, contact insurance carrier to determine if there are any required controls. Evaluate compliance with those controls.

---

<sup>3</sup> Obtain the vendor's assessment of potential weaknesses of their delivery services as well as the controls they recommend and evaluate any mitigation services they provide (the vendor's analysis is only one part of the institution's own analysis).

## **P2. Rate each customer (or type of customer) that performs online transactions.**

It is important to know the level of risk associated with customers using online banking services and especially to know those customers that are high risk. While the focus of these best practices are on corporate accounts that perform online wire and ACH transactions, any customer with any online transaction capability (including bill payments) should be evaluated for risk. Additionally, the FFIEC Supplemental Guidance applies to both business and consumer accounts. Reviews for risk rating customers should be conducted at least annually and documented. There are many different methods and formats that can be used based on the institution's size and resources. An institution may choose to simply rate all consumer customers using bill payment services with low transaction amounts and a low volume limit at a lower risk category than corporate customers. Another option would be to rate as high risk all corporate customers with certain online capabilities. In this case, "individually documented" reviews to determine the risk rating of each customer would not be necessary. However, institutions with a moderate or small number of corporate customers may choose to rate their customers individually.

The following criteria could be used for risk rating a customer:

1. Type of business:
  - a. Domestic versus International; and
  - b. Retail versus wholesale;
2. Average Account Balances (loans and deposits);
3. Services Utilized:
  - a. Wire transfer;
  - b. ACH debit origination files<sup>4</sup>;
  - c. ACH credit origination files; and
  - d. Bill payment;
4. Standard Entry Class (SEC) codes assigned to customer's transactions<sup>5</sup>;
5. Volume of transactions<sup>6</sup>;
6. File Limits/Frequency<sup>7</sup>;
7. Security measures the business account holders utilize (see section P4 below); and
8. Business account holder's administrative controls over their users and system configurations.<sup>8</sup>

## **P3. Outline to the Board of Directors the Corporate Account Takeover issues.**

The Board of Directors should be informed of the risks and controls related to Corporate Account Takeovers and provided with examples of the highest risk customers. This can be accomplished through the following actions.

1. Provide a general description of this crime, how it occurs, and losses experienced in California and the United States<sup>9</sup>.
2. Provide a list of high risk business account holders with their estimated exposure.
  - a. If all account holders have not been risk rated when the report to the Board is made, specify a few of the business customers at greatest risk or list an approximate number of business account customers in the institution's highest category of risk.

---

<sup>4</sup> Debit files could be used to "fund" a theft from the same account.

<sup>5</sup> SEC codes such as PPD (Prearranged Payment and Deposit Entry) and CCD (Cash Concentration and Disbursement) could have more risk than other transaction codes.

<sup>6</sup> Thefts are easier to hide among a high volume of transactions.

<sup>7</sup> Establishing file limits and frequency are a NACHA requirement and help quantify financial exposure.

<sup>8</sup> FFIEC supplemental guidance establishes a minimum expectation regarding enhanced controls for system administration. See section P6 for further details. Administrative controls are of such extremely high risk that if a institution chooses to permit a customer to make administrative changes such as adding new general users, adding administrative users, changing transaction and approval limits, changing passwords, changing customer contact number or method, and disabling notification options, the changes should not be implemented without verification by the institution or at least without notification to the customer (preferable by an out-of-band method) that a change has been made.

<sup>9</sup> An Internet search for "account takeover law suits" will provide numerous articles with examples of these thefts.

- b. If the list of applicable account holders is large, provide summary information and a few examples.
3. Describe the primary measures the institution will be implementing, or has already implemented within the Protect, Detect, and Respond framework.
4. Discuss the action plan and time frames for fully implementing each portion of the Protect, Detect, and Respond framework and for implementing the controls that are needed to meet the minimum expectations in the FFIEC Supplemental Guidance.

#### **P4. Communicate basic online security practices for corporate online banking customers.**

The vast majority of cyber-thefts begin with the thieves compromising the computer(s) of the business account holders. Perpetrators often monitor the customer's email messages and other activities for days or weeks prior to committing the crime. The corporate customer is most vulnerable just before a holiday when key employees are on vacation. Another risk period is on a day the business office is relocating or installing new computer equipment. Employees may be distracted and think a problem conducting online banking is due to a new network or equipment. Therefore it is important and necessary for the corporate customer's employees to follow established security practices. The institution should periodically communicate to the business account holders some or all of the following security practices that the business can implement to reduce their risks of theft. Basic practices to implement include:

1. Provide continuous communication and education to employees using online banking systems. Providing enhanced security awareness training will help ensure employees understand the security risks related to 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 practices);
4. Communicate to employees that passwords should be strong and should not be stored on the device used to access online banking;
5. Adhere to dual control procedures;
6. Use separate devices to originate and transmit wire/ACH instructions;
7. Transmit wire transfer and ACH instructions via a dedicated and isolated device<sup>10</sup>;
8. Practice ongoing account monitoring and reconciliation, especially near the end of the day;
9. Adopt advanced security measures by working with consultants or dedicated IT staff; and
10. Utilize resources provided by trade organizations and agencies that specialize in helping small businesses. See [Appendix A](#) for a list of resources.

#### **P5. Implement/Enhance customer security awareness education for retail and high risk business account holders.**

The FFIEC Supplemental Guidance states that security awareness education should address both business and retail account holders. The effectiveness of the education program and the need for updates due to changes in technology products and security threats should be evaluated at least annually, if not more frequently due to the ever evolving nature of cyber-crime. The extent of security awareness education may vary between customers with different risk ratings. Options for contacting customers include one-on-one or small group meetings, postal mail, email, notices on the institution's website, and telephone calls. Presentations at civic organizations will also be beneficial. Several security and audit vendors as well as trade associations in California have already developed presentation programs. Additionally, a sample presentation for educating account holders is available at [www.dfi.ca.gov/resources](http://www.dfi.ca.gov/resources).

In addition to the basic online security practices mentioned in section P4 above, security awareness education for both retail and business customers could include:

---

<sup>10</sup> Block access to web surfing, social network sites, and external e-mail and any activity not related to banking.

1. Procedures or user guidelines for using the institution's corporate internet banking service;
2. System security features that are available and/or that have been implemented;
3. Procedures to alert institution staff (including specific phone numbers and departments) when the account holder suspects a problem;
4. Policy regarding when, why and how the institution will contact online banking customers<sup>11</sup>;
5. Protections provided and applicability of Regulation E to electronic funds transfers and the types of accounts with Internet access<sup>12</sup>;
6. Common security threats and actions to take in order to prevent, detect, and respond to those cyber-threats (See [Appendix B](#) for examples);
7. Security education resources for the customer (See [Appendix A](#)) and resources that help customers keep abreast of new and emerging issues, such as online security magazines and security vendor websites;
8. Developing an incident response plan (See [Appendix C](#)); and
9. Applicability of laws and regulations to business owners to safeguard information. (See [Appendix D](#)).

Additionally, high risk customers should be specifically contacted and made aware of their exposure to electronic theft. In particular, they should be made aware of:

1. Corporate account takeovers and cyber-thieves;
2. Exposure risks;
3. Recommended minimum security measures to implement (See P4 above);
4. Benefits of the business performing a risk assessment regarding online payment services;
5. Insurance coverage needs related to electronic thefts; and
6. Other resources available on this topic are found in [Appendix A](#).

## **P6. Establish institution controls to mitigate risks of corporate account takeovers.**

It is important to remember that no single control is effective. The FFIEC Supplemental Guidance establishes expectations for layered security controls which should include, at a minimum, the following two elements for both business and consumer accounts.

1. Processes to detect anomalies and respond to suspicious activity<sup>13</sup> related to:
  - a. Initial login and authentication for access to online banking; and
  - b. Initiation of transactions to transfer funds to other parties.
2. Enhanced controls for system administrators who can change access privileges, add users, change or reset passwords, add new payees, change transaction limits, change time of day access, register new access devices, etc.

Institutions will need to work with their IT vendors to ensure that these two elements are in place or will be within a satisfactory time period.

Layered security consists of multiple controls, which may include:

1. Enhanced controls over account administration (an FFIEC minimum expectation) may include:
  - a. Requiring an additional authentication prior to implementing the change;
  - b. Requiring verification/confirmation of changes prior to implementing them;

---

<sup>11</sup> Reiterate that the institution will not request account holders to click on links, install software, or require changes to established procedures without securely communicated notification. (Ensure that policy prohibiting this practice has been adopted to help ensure conformance.)

<sup>12</sup> It is critical that customers understand the different applicability for business/commercial accounts versus personal accounts.

<sup>13</sup> Account monitoring and fraud detection systems should flag transactions for further review. These systems could consider customer transaction history and transaction behavior, including pattern recognition that compares transactions to historical files, unusual amounts, unusual destinations (especially foreign recipients if the customer does not engage in international business), and changes in routing and account numbers of usual recipients (even when the recipient name is not changed). Changes to established cumulative daily limits or transactions in excess of established limits should also be identified by fraud systems as potentially fraudulent activity.

- c. Providing automatic customer notification (such as a text message or automated voice call to a cell phone) immediately after implementing an administrative change;
  - d. Preventing account holders from creating administrative users without institution approval; and
  - e. Eliminating all self-administration if the corporate customer doesn't meet minimum security standards established by the institution;
2. Screen display that shows customers the number of failed logins since the prior successful login and the date and time of their last login;
  3. Fraud-detection and monitoring systems;
  4. Dual customer authorization through different access devices;
  5. Out-of-band verification of transactions (to/from a different access device);
  6. Techniques to restrict transactions such as debit blocks, and debit filters;
  7. Restrictions on account activity such as reasonable limits (based on historic 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;
  8. Tools that block connection from IP addresses known or suspected to be associated with fraudulent activities;
  9. Policies to address potentially compromised customer equipment;
  10. Enhanced controls (similar to those in #1 above) 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;
  11. Customer security awareness education;
  12. Use of USB devices that are read only and which function independently of the customer's computer's operating system, ensuring a secure connection to the institution's network; and
  13. Enhanced challenge questions<sup>14</sup> which would:
    - a. Use sophisticated questions ("out of wallet" information that isn't publically available);
    - b. Require more than one question be answered correctly;
    - c. Include "trap" questions which the customer would recognize as nonsensical and clearly know the answer but a thief could easily guess a wrong answer<sup>15</sup>;
    - d. Establish a large pool of challenge questions; and
    - e. Prohibit the exposure of all challenge questions during one session.

For internal protection, the institution should ensure, at a minimum, the following controls:

1. An effective firewall and a process to evaluate, monitor, and validate firewall settings (and revise if necessary) on an appropriate schedule;
2. An effective patch management program that assesses patch effectiveness and implementation at least monthly; and
3. Additional security measures for computers used internally to access or manage the cash management system should include many of the controls recommended for customers that are listed in section P4.

## **P7. Review customer agreements.**

Signed written agreements should be maintained with corporate customers using online banking services. Given the growing risks of corporate account takeovers, institutions should have legal counsel that is familiar with corporate account takeover risks review their written agreements and consider including the following:

1. Roles and responsibilities for processing transaction requests and dispute resolution;
2. Minimum security standards that the institution requires the corporate account holder to use<sup>16</sup>;

---

<sup>14</sup> The FFIEC's Supplemental Guidance on Internet authentication dated June 28, 2011 states that financial institutions should no longer consider basic challenge questions an effective primary control.

<sup>15</sup> A trap question (also known as a "Red Herring" question) could be something like the following for a customer that never lived in Sacramento, California: *When did you live in Sacramento, California? A) 1976; B) 1980; C) 1983; D) None of the above.* Any answer other than D is a strong indication that the customer's account has been compromised and appropriate institution and customer personnel should be alerted.

3. A disclaimer and acknowledgement that no list of security practices can be all inclusive and foolproof for preventing theft;
4. The establishment of exposure limits through transaction limits, transaction frequencies, and types of payments that can be processed during the customer's normal course of business. Also consider:
  - a. Including the process for changing limits;
  - b. Including a provision authorizing the institution to not honor a transaction request if the institution in its sole discretion believes not processing it will protect the account holder from fraud (include examples that might indicate a transaction is fraudulent); and
  - c. Making an annual disclosure of the account agreement terms, mentioning any changes, and including a pamphlet on security awareness;
5. A disclaimer (absent any warranty or indemnification) that the risk of loss resides with the account holder if a fraudulent payment order is received by the institution in compliance with the institution's normal security procedures;
6. Requirement that the customer provide a list of the employees that are authorized to initiate files, or if the account holder is controlling account administration and accessibility then an acknowledgement from the customer of their responsibility and liability; and
7. Provisions for settling contract disputes. Consider requiring arbitration to settle contract disputes, or include a provision that provides the account holder with warranties or indemnification against corporate account takeover thefts, providing the account holder has followed specific practices.

**P8. Contact your vendors to regularly receive information regarding reducing the risk of corporate account takeovers.**

Corporate account takeovers are a persistent threat and the techniques to commit this crime will continue to be modified. Annually ask your vendors what controls they offer to reduce account takeover risks. Document this as part of the institution's annual risk assessment.

---

<sup>16</sup> The written agreement could also include security procedures offered to the customer.

## **II. Detect**

Detection primarily occurs through:

1. Automated or manual monitoring systems;
2. Institution employee awareness; and
3. Notification from customers (that are aware of symptoms of computer breaches).

Management should evaluate all detection options to implement those which are most practical. Detection is closely associated with protection, as some measures to protect against electronic theft will also be an indication that a theft is being attempted.

### **D1. Establish automated or manual monitoring systems.**

Account monitoring can help detect a theft before money is actually transferred. The most effective automated monitoring systems implement behavior-based transaction monitoring, sometimes called pattern recognition. As outlined in P6 above, the FFIEC Supplemental Guidance expects institutions to implement, at a minimum, processes to detect anomalies related to initial login to online banking and initiation of transactions to transfer funds to other parties.

Things to evaluate:

1. Is the volume of corporate online banking transactions low enough for manual reviews?
  - a. If so, are sufficient personnel (both as primary and as backup) available?
  - b. Can institution personnel develop manual procedures in a reasonable time period that evaluates key red flags listed in section D2 below?
2. Do current vendors offer or plan to offer automated transaction monitoring?
  - a. If so, will the monitoring detect the possible red flags listed in section D2 below?
  - b. What additional features or benefits do the vendors provide?
  - c. Can services be implemented within a reasonable time period?
  - d. How long does it take for the system to build a reliable pattern (predictive analytics) of activity to identify an anomaly?
  - e. Although less reliable than predictive analytics, is rule based fraud analysis available until a behavior pattern of data is established?
  - f. Does any behavior pattern analysis include monitoring account holder online behavior, such as keystroke speed, in addition to time of day activity or transaction based factors.
  - g. Is potential structuring of transactions above preset limits detected as well as unusual frequency of transactions and abnormal time of activity (day of week and time of day)?
3. If current vendors do not offer automated monitoring, are there third-party vendor systems that will integrate with the institution's current systems?
4. How are institution personnel notified if an automated system detects an anomaly?
  - a. Are "suspicious" transactions blocked until an employee releases them?
  - b. Do employees receive notification in a timely manner?

Transaction monitoring for large transactions is one of the most effective techniques for detecting fraudulent transactions. Institutions with a limited number of corporate account holders can implement manual reviews and block suspicious transactions (or obtain further confirmation from their customer). A checklist of characteristics to review, such as those in D2, should be part of any manual review procedures to help ensure consistent evaluations.

## **D2. Educate institution employees of warning signs that a theft may be in progress.**

Employee awareness is essential in the detection of fraudulent account activity. Employees are generally the first and last line of defense. Employees with corporate account holder contact and especially those that process ACH and wire transactions need to know the types of customer inquiries and other warning signs that could indicate a theft is underway. They should be aware that any problems customers are having accessing or contacting the institution electronically might be a multi-prong attack to either divert the institution's attention from a theft in progress or to disrupt communications between the customer and the institution while the theft is occurring. Reviewing transaction security reports for unusual volume and dollar amounts is helpful and should be performed at least daily as some thefts occur over multiple days. However, this method only identifies a fraud after funds have left the institution.

A sample presentation to aid in educating institution employees is available at [www.dfi.ca.gov/resources](http://www.dfi.ca.gov/resources).

Red flags visible to the institution of a possible takeover of a business account include:

1. Configuration changes to cash management/online banking profiles:
  - a. New user accounts added;
  - b. New ACH batches or wire templates with new payees;
  - c. Changes to personal information;
  - d. Disabling or changing notifications; and
  - e. Changes to the online account access profile;
2. Unusual customer activity<sup>17</sup>:
  - a. Unfamiliar IP log-on address (especially if a foreign IP address);
  - b. Device ID not recognized during any previous log-on;
  - c. Log-on and/or viewing of balance or transaction history during unusual times of days;
  - d. Unusually small transaction amounts (example: \$1.00 ACH, bill pay, or other transactions – especially if made at unusual time of day);
  - e. Unusual non-monetary request from customer via fax, email, or cash management system;
  - f. Unusual (non-typical) transfer of funds, especially if out of the institution. One-time bill pay to new payees;
  - g. ACH or wires to new payees or receivers and/or with unusual amounts;
  - h. Changes to the account and routing numbers of existing payees, not just a new payee name;
  - i. Unusual timing of transactions (based on the established transaction schedule of the corporate customer or random transactions submitted between traditional transactions);
  - j. Larger than usual transactions; and
  - k. Overseas transfers;
3. Compromised internal systems used by institution employees resulting in:
  - a. Inability to log into online banking system (thieves could be blocking the institution's access while they are making modifications to account settings);
  - b. Dramatic loss of computer speed;
  - c. Changes in the way web pages, graphics, text or icons appear;
  - d. Computer lock up so the user is unable to perform any functions;
  - e. Unexpected rebooting or restarting of computer;
  - f. Unexpected request for a one time password (or token) in the middle of an online session;
  - g. Unusual pop-up messages, such as "try back later" or "system is undergoing maintenance";
  - h. New or unexpected toolbars and/or icons; and
  - i. Inability to shut down or restart.

---

<sup>17</sup> Generally, hackers will have done some type of monitoring/transaction testing of the corporate account before a monetary theft is made.

In the event that any of the above items are noted, the institution's network administrator and/or the online banking system operator should be contacted for further investigation.

**D3. Educate account holders of warning signs of potentially compromised computer systems.** (This is similar to educating institution employees.)

Account holders should be the most vigilant in monitoring account activity. They have the ability to detect anomalies or potential fraud prior to or early into an electronic robbery. If your institution offers some of the automated notification features mentioned in P6, remind your customers those are designed as flags for them to notify you if they think they may have been compromised. Business account holders should be alert for the same red flags related to computer and network anomalies as institution employees.

Warning signs visible to a business or consumer customer that their system/network may have compromised include:

1. Inability to log into online banking (thieves could be blocking customer access so the customer won't see the theft until the criminals have control of the money);
2. Dramatic loss of computer speed;
3. Changes in the way things appear on the screen;
4. Computer locks up so the user is unable to perform any functions;
5. Unexpected rebooting or restarting of the computer;
6. Unexpected request for a one time password (or token) in the middle of an online session;
7. Unusual pop-up messages, especially a message in the middle of a session that says the connection to the institution's system is not working (system unavailable, down for maintenance, etc.);
8. New or unexpected toolbars and/or icons; and
9. Inability to shut down or restart the computer.

### **III. Respond**

#### **R1. Update incident response plans to include corporate account takeover.**

An incident response plan should include actions for stopping a corporate account takeover and should be reviewed at least annually. Update the plan to include the following:

1. Designate a fraud response committee with a specific member as the central point of contact for cyber-threats. Ensure that:
  - a. All institution employees know that any phone calls from customers that might be about a corporate account takeover must be transferred to the designated employee as soon as possible;
  - b. The designated employee knows to convene the fraud response committee to evaluate the situation and take appropriate action;
  - c. The designated employee has been given authority to take immediate action and reverse or block suspected transactions;
  - d. Multiple backup personnel are in place in the event that the designated employee is unavailable. (These thefts exploit reduced staffing of holiday and vacation periods.); and
  - e. Account holders have provided a primary and secondary contact person along with afterhours phone numbers that the institution can call to confirm activity that appears suspicious;
2. Identify the recovery time frame and resources needed, including:
  - a. Number of employees available and trained to attempt to recover the money;
  - b. Resources/skills needed by the designated central point of contact at the institution; and
  - c. Resources needed by the recovery team;
3. Address customer relations/communication during an incident. Include these steps:
  - a. Identify the institution staff permitted to speak to the customer;
  - b. Script the initial employee communication with the customer;
  - c. Confirm account holder is aware that the institution is not automatically accepting liability; and
  - d. Identify the institution staff permitted to speak to the media;
4. Include criteria for contacting computer forensic specialists to review appropriate equipment as well as contact information; and
5. Include and maintain contact information for all regulatory agencies, the United States Secret Service and other law enforcement agencies. They should be contacted as early as possible but without diverting resources from the initial recovery effort.

#### **R2. “Immediately” verify if a suspicious transaction is fraudulent.**

Institution employees should know how to contact account holder immediately. The customer’s primary and secondary contact information including after-hours phone numbers are critical, not email addresses.

#### **R3. “Immediately” attempt to reverse all suspected fraudulent transactions.**

An institution’s ability to recovery funds is reduced over time, measured in minutes, not hours. Thefts often include both wire transfer and ACH transfers, and could include other forms of transfers in the future. Be prepared to address all types. Have software available for immediate use to edit ACH files either onsite or through your correspondent or online banking vendor.<sup>18</sup> Be aware that the FRB has different “processing times” for transactions and reversals. Reversals are sometimes not processed until hours or days after a transaction has already been sent and it is too late to recover the funds. No

---

<sup>18</sup> Some online banking systems create ACH files that include a large number of different customers. The ability to edit the file to remove fraudulent transactions so that the file can be sent for processing of the legitimate transactions of other customers is important. Often the fraudulent transactions occur near the cutoff time when there is not sufficient time to manually re-enter all of the legitimate transactions.

fraudulent transactions should be sent for processing along with a reversing entry under the presumption that the “reversal” will cancel the processing instruction.

#### **R4. Send a “Fraudulent File Alert” through FedLine.**

Sending a “Fraudulent File Alert” through the FRB’s FedLine system may help prevent receiving institutions from delivering funds to their customer (who is receiving stolen funds). In 2011 there were three steps to file an alert:

1. Contact the FRB Operations Center;
2. Fax or email the information to the FRB; and
3. Follow up to confirm the alert had been transmitted by the FRB.

FRB contact information and a sample form for notifying the FRB are included in [Appendix E](#).

#### **R5. “Immediately” notify the receiving institution(s) of the fraudulent transactions and ask them to hold or return the funds.**

Once cyber-thieves have transferred the stolen money to another institution, the thieves will attempt to move the money out as rapidly as possible. A process/plan must be in place for notifying the institution(s) that has received the stolen money and requesting a hold on those funds. The following steps should be taken:

1. Locate phone numbers for institutions ACH departments using the FRBs FedACH directory at [http://www.fededirectory.frb.org/search\\_ACH.cfm](http://www.fededirectory.frb.org/search_ACH.cfm);
2. Distribute the list of fraudulent transactions to a group of institution employees with calling assignments and instructions to call on the largest items first. Distribute the largest transactions among several employees to facilitate the quickest call-back on the largest transactions;
3. Remind institution employees making the phone calls that the employee at the receiving institution is crucial to recovery. If recovery effort is occurring after normal business hours or extends beyond normal business hours, ask the employee at the receiving institution for an after-hours phone number in case a call back is needed;
4. Document all calls with names, dates, and times; and
5. Send a notice of fraudulent activity to the receiving institution(s). A sample form is available at [www.dfi.ca.gov/resources](http://www.dfi.ca.gov/resources). This sample form is **not** endorsed, recommended or required by the California Department of Financial Institutions. It is provided because it may be useful as a starting point in drafting an appropriate notice of fraudulent activity, with the assistance of institution counsel.
6. If the receiving institution sees that a “Fraudulent File Alert” has arrived from the FRB, they may have greater confidence that not delivering the funds to their customer will not result in liability from their customer; and
7. If the receiving institution employee is reluctant to hold the funds, remind them that this is a theft and minutes are crucial in preventing the theft from being successful. Request to speak to a supervisor.

#### **R6. Implement a contingency plan to recover or suspend any systems suspected of being compromised.**

When a system is suspected of being compromised, it is important to close off the method being used to commit the crime.

1. If it appears that user credentials of your customer have been compromised, consider immediately disabling your account holder’s access to the online banking system.

2. If it appears that the institution's network was compromised, consider shutting down all online corporate banking activity (if that is feasible).
3. Depending on the size of the theft and potential losses, consider having forensic analysis performed on all suspected compromised systems as soon as possible to determine where, when and how the compromise occurred<sup>19</sup>. Consider paying for the analysis of your account holder's system to help in the institution's discovery of how the crime was committed.

### **R7. Contact law enforcement and regulatory agencies once the initial recovery efforts have concluded.**

Law enforcement and regulatory agencies should be contacted once initial recovery efforts are complete. Have these agency contact numbers available in advance. In addition, a Suspicious Activity Report must be filed with the Financial Crimes Enforcement Network (FinCEN). Agencies to contact include:

1. United States Secret Service (or other federal law enforcement agency)<sup>20</sup>;
2. State and local law enforcement; and
3. State and federal financial institution regulatory agencies.

### **R8. Implement procedures for customer relations and documentation of recovery efforts.**

Since the account holder can be the victim of a large theft, proper handling of the incident is important for customer relations, financial liability, and potentially public relations. Procedures should be in place regarding contacting customers and documenting all discussions. It is important to keep in mind that when an electronic theft is initially discovered, the source of the compromise is sometimes unknown.

1. Designate one employee in the institution as the central point of contact for communicating with the account holder and have a prepared script of the actions the institution is taking to retrieve their funds.
2. Document account holder discussions (note names, date, and times), especially how and when the account holder believes the compromise began.
3. Reassure account holders that the institution is diligently working towards a full recovery of the funds; however, there is no guarantee that a full recovery will be achieved.

---

<sup>19</sup> The institution's contingency plan needs to include the names of the firms to use for forensic analysis as well as primary and secondary contacts and after hours phone numbers. Perform a review of these vendors in advance. There isn't time to find or fully evaluate a company when a situation occurs. Trade associations and other technology related service-providers may be a good reference source.

<sup>20</sup> Contact your local United States Secret Service field office ([http://www.secretservice.gov/field\\_offices.shtml](http://www.secretservice.gov/field_offices.shtml)) or the Secret Service's local Electronic Crimes Task Force (<http://www.secretservice.gov/ectf.shtml>). Contact information for the local FBI field office can be found at <http://www.fbi.gov/contact-us/field/field-offices>. You may also want to file a complaint with the Internet Crime Complaint Center ([www.ic3.gov](http://www.ic3.gov)).

## **RELATED ISSUES – MONEY MULES**

### **Identifying Potential Money Mule Activity<sup>21</sup>**

While it is important to prevent and detect thefts from your own corporate customers' accounts, it is also important to monitor for thefts that might be passing through your institution through a money mule account.

Warning signs that an institution customer could potentially be a money mule include:

1. New accounts opened with small deposit followed shortly by larger transfers via ACH or wire;
2. J-1 Visa student accounts receiving (unusually) large transfers;
3. New/unusual sources of transferred funds;
4. An existing account with a sudden increase in the number and dollar amount of deposits by ACH credit or wire transfer;
5. An account that receives a large deposit followed by an immediate withdrawal, or around 10% less than the original deposit; and
6. Destination of the monetary transfer that is not typical for the customer.

### **Internal Controls**

Certain internal controls can be implemented should your institution be used to move stolen money through a money mule account. Consider the following controls:

1. Establish a central point of contact (and backup) for working with other institutions that have account holders that have been victimized;
2. Determine how holds, returns and withdrawals/transfers will be allowed;
3. Determine what documentation will be required before holding or returning funds;
4. Evaluate the history of the account holder that is receiving the potentially stolen funds to determine if the incoming transactions are consistent with prior history; and
5. Identify any red flags indicating that the account is or has become a "money mule" account (see above).

---

<sup>21</sup> Evaluate policies for options to close accounts used to transfer stolen funds to thieves, commonly called "money mule" accounts. Educate institution employees on the characteristics of money mule accounts. Money mules are often existing account holders that have been recruited through postings of legitimate sounding job offers on popular Internet job sites. However, the "employer" (cyber thief) asks the money mule to receive and then quickly transfer money to another institution; money mules are involved in money laundering; and money mules may claim to be unaware (and in some cases may actually be unaware) that they are facilitating a theft.

## APPENDIX A

### Resources for Business Account Holders

1. The Better Business Bureau's website on Data Security Made Simpler: <http://www.bbb.org/data-security> ;
2. The Small Business Administration's (SBA) website on Protecting and Securing Customer Information: <http://community.sba.gov/community/blogs/community-blogs/business-law-advisor/how-small-businesses-can-protect-and-secure-customer-information>;
3. The Federal Trade Commission's (FTC) interactive business guide for protecting data: <http://www.ftc.gov/bcp/edu/multimedia/interactive/infosecurity/index.html>;
4. The National Institute of Standards and Technology's (NIST) Fundamentals of Information Security for Small Businesses: <http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf>;
5. The jointly issued "Fraud Advisory for Businesses: Corporate Account Takeover" from the U.S. Secret Service, FBI, IC3, and FS-ISAC available on the IC3 website (<http://www.ic3.gov/media/2010/CorporateAccountTakeOver.pdf>) or the FS-ISAC website (<http://www.fsisac.com/files/public/db/p265.pdf>); and
6. NACHA – The Electronic Payments Association's website has numerous articles regarding Corporate Account Takeover for both financial institutions and customers: [http://www.nacha.org/c/Corporate\\_Account\\_Takeover\\_Resource\\_Center.cfm](http://www.nacha.org/c/Corporate_Account_Takeover_Resource_Center.cfm).

## APPENDIX B

### Examples of Deceptive Ways Criminals Contact Account Holders

1. The FDIC and the NCUA do **not** directly contact institution customers (especially related to ACH and Wire transactions, account suspension, or security alerts), nor does the FDIC or NCUA request institution customers to install software upgrades. Such messages should be treated as fraudulent and the account holder should permanently delete them and not click on any links.
2. Messages or inquiries from the Internal Revenue Service, Better Business Bureau, NACHA, and almost any other organization asking the customer to install software, provide account information or access credentials is probably fraudulent and should be verified before any files are opened, software is installed, or information is provided.
3. Phone calls and text messages requesting sensitive information are likely fraudulent. If in doubt, account holders should contact the organization at the phone number the customer obtained from a different source (such as the number they have on file, that is on their most recent statement, or that is from the organization's website). Account holders should not call phone numbers (even with local prefixes) that are listed in the suspicious email or text message.

## **APPENDIX C**

### **Incident Response Plans**

Since each business is unique, customers should write their own incident response plan. A general template would include:

1. The direct contact numbers of key institution employees (including after hour numbers);
2. Steps the account holder should consider to limit further unauthorized transactions, such as:
  - a. Changing passwords;
  - b. Disconnecting computers used for Internet banking; and
  - c. Requesting a temporary hold on all other transactions until out-of-band confirmations can be made;
3. Information the account holder will provide to assist the institution in recovering their money;
4. Contacting their insurance carrier; and
5. Working with computer forensic specialists and law enforcement to review appropriate equipment.

## **APPENDIX D**

### **Information Security Laws and Standards Affecting Business Owners**

Although institutions are not responsible for ensuring their account holders comply with information security laws, making business owners aware of consequences for non-compliance if the information is breached can reinforce the message that they need to maintain stronger security. Breaches of credit and debit card information from retail businesses are common. Loss of that information or sensitive personal information can create financial and reputational risks for the business.

When providing security awareness education to corporate customers, institutions may want to also alert business owners of the need to safeguard their own customers' sensitive information. California statutes related to safeguarding customer information include:

- Sections 1798.80-1798.84 of the California Civil Code, which was enacted to ensure that personal information about California residents is protected.

The Payment Card Industry Security Standards Council was launched in 2006 to manage security standards related to card processing. Any merchant that accepts credit or debit cards for payment is required to secure their data based on the standards developed by the council. The PCI Security Standards Council's website [https://www.pcisecuritystandards.org/security\\_standards/index.php](https://www.pcisecuritystandards.org/security_standards/index.php) notes that noncompliance may lead to lawsuits, cancelled accounts, and monetary fines. The website provides information for small business compliance.

## APPENDIX E

### Procedures for Sending a Fraudulent ACH File Alert Request to the Federal Reserve Bank

The following information is valid as of September 2011. Institutions should update their FRB contact information at least annually as part of updating their incident response plan.

1. **Contact FRB Operations and/or your representative with the Federal Reserve.**

Contact information for FEDACH Central Operations Support can be located on the Federal Reserve Bank Services website @ [www.frbservices.org/contactus/fedach\\_operations.html](http://www.frbservices.org/contactus/fedach_operations.html).

Contact information for FRB San Francisco Account Executives can be located on the Federal Reserve Bank Services website @ [www.frbservices.org/contactus/sales\\_account\\_executives.html#sanfrancisco](http://www.frbservices.org/contactus/sales_account_executives.html#sanfrancisco)

2. **Fax or email the following information to your Federal Reserve contact.**

The following sample form is **not** endorsed, recommended or required by the California Department of Financial Institutions. It is provided because it may be useful as a starting point in drafting an appropriate fraudulent ACH file alert, with the assistance of institution counsel and your Federal Reserve contact.

### SAMPLE MESSAGE

A FRAUDULENT file was processed for \_\_\_\_\_ (*Institution Name & ABA*) in error on \_\_\_\_\_ (mm/dd/yy). The original file was processed on \_\_\_\_\_ (mm/dd/yy) with settlement of \_\_\_\_\_ (mm/dd/yy). The FRAUDULENT file was processed on \_\_\_\_\_ (mm/dd/yy) and will settle on \_\_\_\_\_ (mm/dd/yy). A reversal file was processed on \_\_\_\_\_ (mm/dd/yy) and will settle on \_\_\_\_\_ (mm/dd/yy). For additional information, contact \_\_\_\_\_ (*Institution Name*) at \_\_\_\_\_ (*Institution's phone number*).

\_\_\_\_\_ (*Institution Name & ABA*) hereby assumes all responsibility and liability for any processing errors, losses, damages, and liability in any way arising out of the transmission of the broadcast message.

\_\_\_\_\_ (*Institution Name & ABA*) also agrees to indemnify and hold harmless the Federal Reserve Bank, its agents and employees, from and against all claims, damages, lawsuits, and expenses, including reasonable attorneys' fees, in any way arising out of the transmission of the broadcast message.

3. **Follow up and confirm that the message has been transmitted.**