
# FS-ISAC
# Account Take Over Task Force:

# Account Take Over
# and
# Online Fraud Response
# White Paper

Version: 1.0

**This white paper is a publication of the Account Take Over Task Force, a collaborative cross-industry effort to develop and distribute sound business practices to prevent, detect and respond to Corporate Account Take Overs.**

**DATE PUBLISHED: JUNE 17, 2011**

**TABLE OF CONTENTS**

**FS-ISAC ACCOUNT TAKE OVER TASK FORCE: ACCOUNT TAKE OVER AND ONLINE FRAUD RESPONSE WHITE PAPER**

# 1. Document Information

## *1.1. Purpose*

This document is intended to be used by financial institutions as a guideline to assist in developing a response strategy for account take over events.

## *1.2. Scope*

Financial institution's using on-line banking applications.

## *1.3. Contributors*

| Name | Title |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## *1.4. Change History*

| Changes | Date | Version |
|---|---|---|
| Initial Release | June 17, 2011 | 1.0 |
| | | |
| | | |

## *1.5. Information Classification*

The FS-ISAC uses an information classification policy. This whitepaper is classified as FS-ISAC GREEN meaning that its contents may be shared with FS-ISAC members, partners, and other ISACs. It is not to be shared freely or posted for viewing on public websites.

# 2. Account Take Over Response Guidelines

This document should be used by financial institutions as a guideline to assist them in creating a more detailed strategy for responding to account take over events that typically result from malware infections. This document is meant to provide specific guidance to address a specific type of fraud (account take over).

Implementation of the recommendations within this document will vary depending on the size and complexity of the financial institution. Please understand this document acts as a guideline and each financial institution should evaluate how to best leverage its contents.

Since institutions are organized differently, efforts were made to use generic job titles so the document can be tailored to meet an individual institution's needs.

## *2.1. Background*

Malware (malicious software) is a significant computer-related problem impacting financial institutions and their customers. The sole purpose of the creators of malware is to obtain financial benefit from its distribution; consequently, malware can take on multiple forms such as worms, viruses, spyware, or Trojans. Malware is aggressive and sophisticated, often using a combination of techniques to accomplish its malicious purpose.

Spyware, Trojans, and key loggers are popular with criminals, including organized crime. These malicious programs can be used to obtain users' online credentials through the infected computer, and other information such as account numbers, PINs, and other sensitive account data through email and internet browsing activity. The resulting data can be sold or used directly to perpetrate fraud.

Consequently, the FS-ISAC formed the Account Take Over Task Force. The Task Force has developed this white paper to assist financial institutions in implementing a response strategy once an account take over has been detected for a customer account.

## *2.2. Strategic Planning*

***"He, who fails to plan, plans to fail."***

***Italian Proverb***

Planning ahead and being prepared to respond to an account take over event is the first and most critical step. Your organization should ensure that you have a documented process for responding to account take over situations prior to an

event occurring. Any and all impacted groups or departments should be identified and included in the response process definition and documentation stages. It is important to have a documented playbook that details which responsibilities each department or team has and what role they play in responding to the account take over event. To assist in the development of a response plan, an "Interdepartmental Response Model" was developed and can be found at the FS-ISAC member only web site. The Model provides an overview of two scenarios and lists the potential action steps employees within a financial organization would take to address the event. The action steps are listed in the order of priority. Please note the titles given to the employee roles in this Model may be different from those used at your financial institution. Additionally, be sure to identify which departments are considered "Primary" response team members from those that play a secondary, or support role. Each department or team member identified may have a different role or responsibility. It is important to establish response activities and priorities that work best for your particular institution.

Effective communication is essential to successfully managing response activities.

- Within your response playbook, be sure to identify who will act as a single point of contact and manage all communications with the impacted customer.

- Be aware that incoming communications on these types of events may also come into your organization through other channels, including your branches, call centers, or other business units.

- Communicate to these other business areas ahead of time and consider including them in the response planning discussions, as it will be important for them to know how to identify a potential account take over event and what steps to take.

- Define a standard set of processes that will be used to communicate with other departments or teams involved in the response activities by leveraging e-mail and document templates so complete and consistent information is always collected, reported and shared.

Strategic planning is an ongoing process, not a one-time event. We recommend reviewing and testing your plan at least once a year, and qualifying your plan as a living document.

Financial institutions should already have in place response programs for unauthorized access to customer information and customer notice developed pursuant to section 501(b) of the Gramm-Leach-Bliley Act (GLBA). These GLBA provisions apply to consumer accounts only and the unauthorized access programs may not be applicable or suited toward corporate account take over situations. However, financial institutions may be able to leverage their existing unauthorized access programs or the GLBA regulatory framework when considering and developing a corporate account take over response.[1]

Additionally, financial institutions also have in place money laundering and fraud monitoring programs which may also be leveraged as part of their account take over response.

All financial institutions are encouraged to register annually with FinCEN (Financial Crimes Enforcement Network, United States Department of the Treasury) under the USA PATRIOT Act Section 314(b) which provides a safe harbor from liability and permits financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity. Additional registration information can be found at the following link: www.fincen.gov/statutes_regs/patriot/section314b.html.

Below is a list of items that should be considered when developing your response procedures. Although this list is comprehensive, it should not be considered an all inclusive list and is only intended to help you get started with your planning.

- Determine issues or events where you should involve the customer.
- Determine when user account names and authentication tokens (passwords, certificates, challenge questions, etc.) should be changed.
- Determine when account numbers should be changed.
- Determine when a SAR should be submitted.
- Determine when law enforcement should be involved.
- Define when to disable a customer's online account and how to terminate any active sessions.
- Determine when it is appropriate to reverse or request a return of an ACH transaction or wire transaction.
- Determine handling processes for any fraudulent ACH transactions in a bundled ACH file keeping in mind that all ACH transactions (bundled and unbundled) must flow through the OFAC screening process.
- Determine a process for flagging and forwarding information related to fraudulent ACH transactions and/or bundled ACH files to internal investigators for proper follow-up.
- Define when and if forensics should be performed on the affected computer(s).

---

[1]. See 12 C.F.R. part 30 app. B. (OCC); 12 C.F.R. part 208, app. D-2 and part 225, app. F (Board); 12 C.F.R. part 364, app B (FDIC); and 12 C.F.R. part 570, app. B (OTS).

- Define how to shut down a phishing site related to your financial institution.
- Define how to process recovered user account credentials.
- Determine who in management should be notified.
- Determine when bank regulators should be notified.
- Determine if communications should be sent to all customers (e.g. post advisory messages regarding phishing attempts).
- Determine the actions to follow when a malicious IP address has been uncovered.
- Define how long to block or monitor malicious IP addresses.

## *2.3. Immediate Response*

Once your institution is notified of, or detects, a potential account take over event, it is time to initiate your response plan. The section below outlines activities that should be carried out as quickly as possible to help reduce the risk of loss – or additional loss – for the customer. Many of the steps below will be a coordinated effort and will be carried out by multiple teams. It will be up to each organization to determine how to incorporate these guidelines into their response plans, and who will be responsible for each step. Financial institutions should incorporate the titles of key positions as opposed to using actual named individuals of the organization. This will alleviate paperwork changes that could become necessary with employee attrition.

A case should be opened and assigned to someone for investigation.

- The investigator should immediately identify any other potentially fraudulent transactions already submitted in payment systems (e.g. wire transfer, ACH, bill payment, internal transfers, etc.).
- The investigator should review online activity for the compromised user/account in existing fraud prevention or detection reporting system(s) to determine whether additional fraudulent or suspect activity was flagged for review in other channels or product lines.
- The investigator should provide any pertinent information or unusual transactions to the customer point of contact. All information should be reviewed with the customer to identify fraudulent transactions which need to be stopped or cancelled.

The customer point of contact, sometimes referred to as the Relationship Manager, notifies the customer of the possible account take over event, at which time he advises the customer of the institution's primary point of contact during the event, and validates any pending (or recently completed) transfers. **It is very important for the primary point of contact to keep an open line of communication with the customer throughout the event response process.**

- Use only contact information the bank has used previously or from a core backend system.
- Do not rely on contact information from customer facing applications (i.e., Internet Banking) to contact the customer unless additional due diligence on the contact information has been performed. This data is often manipulated by the cyber criminals.

If the customer confirms the fraud, or that the account is at risk for fraud, disable any existing, impacted online user account(s) immediately, or at a minimum, make sure they are closely monitored during the transition of services. The following actions should be considered and performed as quickly as possible.

- Immediately stop or cancel any open transactions which have not been processed.
- Immediately identify and contact the receiving institution to determine status of any fraudulent transactions processed for settlement. Use the FS-ISAC membership directory to determine fraud contacts at member institutions. Request funds be frozen by the receiving institution as soon as possible. If the receiving institution has concerns, offer to execute a "hold harmless" agreement (indemnity agreement). See your legal counsel for questions and guidance on a "hold harmless" agreement.
    - Pending Transfers - Contact beneficiary's bank to stop payment.
    - Closed Transfers – Contact beneficiary's bank to request funds be returned.
- Terminate any active sessions the customer may have open.
- If possible, place an alert or message on the customer's accounts to ensure other customer service representatives are aware of the potential fraud.
- Determine whether or not the customer processes transactions under dual control and disable any exposed user IDs. (Determining all exposed user IDs may not happen until the investigation is complete.)
- If the administrator ID was not compromised, ask the customer administrator to set up new User IDs after the customer receives approval from the financial institution.
- If the administrator ID was exposed, all IDs should be shut down and replaced, including the administrator ID.
- Instruct the customer to:
    - Remove any PCs suspected (or confirmed) of being infected with malware off of the network immediately;
    - Refrain from using any PCs suspected (or confirmed) of being infected with malware;
    - Replace the hard drive if the PC must be put back into service (formatting the hard drive is not recommended as the malware could be resident in the PC's memory);
    - Secure the infected hard drive for forensic or law enforcement inspection, as needed; and
    - Seek third party assistance to identity all infected devices.
- Advise the customer to change passwords and review transaction activity for all other online accounts (e.g. accounts at other institutions) that might have been compromised by the malware.

You will want to proactively work with the customer if ACH/Wire files need to be originated before a new ID can be created.

## *2.4. Investigation*

While the primary response teams are managing the initial response activities, the support response teams should begin working on other important response related tasks in parallel. The *Investigation* phase is an important phase of the response plan and allows the financial institution an opportunity to glean a significant amount of useful information about the account take over event. The goal is to learn as much as possible about the event - who, what, when, where, why and how. The financial institution can use the information collected during the investigation phase to improve detection and prevention controls, improve response procedures, educate their customers, and mitigate further risk.

When appropriate, work with the customer's point of contact to gather information about how the credentials were compromised. This may include, but is not limited to, talking with the customer as well as other necessary research. Be sure to document the initial customer responses. If an email was the point of infection, ask the customer for a copy of the email (including the header records) and share this information with law enforcement.

Internally, partner with other departments to obtain additional logging information on the fraudulent transactions. Below are some steps that you might consider as part of the investigation phase:

- Engage law enforcement (as appropriate/necessary).
- Mine the account and any associated logs for useful information:
    - Determine the originating IP Address of fraud and perform research to determine if this IP address has been used to access other online banking accounts.
    - Determine if there are any other useful session based anomalies.
    - Determine the beneficiaries of the fraud payment(s).
    - Are there any other payments to the same beneficiary? If yes, follow-up as possible fraud.
    - Are there any other accounts which have been accessed from the IP address used in the fraud?
    - If possible, try to identify any other customer account related information the cyber criminal may have accessed while in the customer's account. This may provide the financial institution an opportunity to identify potential cross-channel fraud exposures.
- Provide beneficiary information and IP addresses to the fraud investigator and law enforcement.
- Perform a risk assessment to determine whether core account numbers have been compromised. If they were compromised, perform the following actions:

    - close existing accounts;
    - open new accounts;
    - change the Internet banking customer profile to the new accounts; and
    - set up existing business services (e.g. ACH, wire transfer, anti-fraud services) on new accounts, if needed.
- If feasible, work with the receiving bank fraud investigator to document how the beneficiary was duped. (Note: Beneficiaries may be innocent victims of the scam or possibly money mules.[2])
    - Ask for any electronic communications that may have transpired with cyber criminals (e-mails, etc.).
        - If available, ask for the original communications in order to obtain the e-mail header information.
    - Try to determine the answers to the following questions and include these details in the suspicious activity report (SAR):
        - Where was the beneficiary asked to send the money?
        - How did the beneficiary make initial contact with the cyber criminals?
        - Did the beneficiary have resumes on job sites like Monster or CareerBuilder?
        - How did the beneficiary withdraw the money (ATM or over the counter)?
        - Was the customer's phone forwarded by the telecommunications provider based on social engineering by the cyber criminals?
        - Was another phone number added by the cyber criminal to the customer's online banking profile?
        - Did the customer respond to a phishing email or a new pop-up requesting personal information, account information, or banking credentials
- If captured from an online take over, add the fraudulent device ID to a "hot-file list" (also known as negative file or fraud database) for potential alerting, further review, or restriction of attempted activity on any subsequently targeted accounts by the same cyber criminal.
- Add the beneficiary to internal payments watch list(s) and other industry watch list databases in which you participate (e.g., fraud list or fraud database).

## *2.5. Remediation*

The *Remediation* phase should begin after all time sensitive response activities have been completed. During the *Remediation* phase, the financial institution should partner with the customer to help them understand how the fraud occurred (when feasible), what steps to take next, and how to better protect themselves in the future. The financial institution should also take this opportunity to educate the customer about additional controls that can be put in place to reduce the

[2]In general, money mules are consumers who have been willingly or unwittingly recruited by the cybercriminals to establish bank accounts that will be used to receive and send out the stolen funds.

likelihood of future account take over events and/or financial losses related to these types of events.

The following activities should be considered for inclusion in the remediation phase.

- Continue working closely with the customer to ensure his banking needs are met during each stage of the response plan.
- Work with the customer to set up new ACH or wire transfer profiles (supply ACH file information / ACH record layout if needed to populate entries).
- Set up a new customer login ID and transfer all existing permissions.
- Open new accounts for the customer and submit paperwork to setup existing Treasury Management services on new accounts.
- Review the online transfer limits and approvals for ACH files and wire transfers. Adjust as appropriate.
- Discuss the following account monitoring fraud and control services with the customer:
    - ACH and Wire Intraday and/or End of Day Reporting;
    - ACH Transaction Control;
        - Blocks
        - Filters
    - Positive Pay;
    - Reverse Positive Pay;
    - Dual control for execution of high value transactions;
    - Out of Band Alerts or call backs;
    - Systematic Alerts requested by the customer (example being an alert sent from the Wire system because the requested threshold was exceeded);
    - Block International Wires/ACH files if the customer never sends international wires/ACHs; and
    - Suggest a separate PC be used for only online banking.
- Notify other applicable lines of business contacts if the customer used those additional services offered by the financial institution (e.g., Investment Advisors/Merchant Processing).
- Have the financial institution's customer point of contact recommend the customer file a report with the Internet Crime Complaint Center (IC3)[3] educate the customer on information security practices, current malicious software concerns, additional recommended controls and possibly additional fraud services.
- Submit any malware/Trojan samples to the local FBI or USSS, even though the case may not meet the threshold for investigation by the FBI or USSS, and to the institution's anti-virus vendor. Additional options for malware submission are under development. FS-ISAC advisories will be issued as these options become available.
- Consider all contact information within the online banking system as possibly fraudulent. Never allow contact information changes via online

[3] Additional information can be found at www.ic3.gov.

banking systems to populate the legacy system without additional due diligence.

# 2.6. External Reporting

## 2.6.1. SARS

It is important that you file any necessary SARs.

The purpose of the Suspicious Activity Report (SAR) is to report known or suspected violations of law or suspicious activity observed by financial institutions subject to the regulations of the Bank Secrecy Act (BSA).

Financial institutions are required to submit SAR forms that are complete, sufficient and in a timely manner. To ensure a consistent reporting process for account take over via a SAR, see recommendations in Appendix 1.

Because the SAR narrative serves as the only free text area for summarizing suspicious activity, it is essential that financial institution employees write narratives that are clear, concise and thorough. See the following link for more information on completing a SAR:
http://www.fincen.gov/news_room/rp/sar_tti.html

The failure to adequately describe the factors making the transaction or activity suspicious undermines the very purpose of the SAR and lessens its usefulness to law enforcement. Late filings, absence of supplemental SARs and/or inaccuracies in SARs have an impact upon law enforcement's ability to determine whether a crime was committed and to what extent the crime may have been committed. Therefore, it is imperative that financial institutions not only file complete and sufficient SARs but that those SARs are filed within required deadlines.

## 2.6.2. Provision of Safe Harbor

Federal law provides complete protection from civil liability for all reports of suspicious activity transactions made to the appropriate authorities, including supporting documentation, regardless of whether such reports are filed in accordance with SAR filing guidelines or on a voluntary basis. Federal law and regulation also provides that a SAR and any information that would reveal the existence of a SAR, are confidential, and shall not be disclosed except to FinCEN or any Federal, State, or local law enforcement agency; or any Federal or state regulatory authority that examines the bank for compliance with the Bank Secrecy Act.

## 2.6.3. Reporting Suspicious Activity

All financial institutions operating in the United States are required to file a suspicious activity report following the discovery of: (1) insider abuse involving any dollar amount; (2) violations aggregating $5,000 or more where a suspect can be identified; (3) violations aggregating $25,000 or more regardless of a potential suspect; and (4) transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act. Although

banks are required to file a SAR when the suspicious activity amounts to $5,000 or more, financial institutions are permitted to file at a lower dollar threshold.

For reporting an account take over via a SAR:

- Check the "other" box with a notation "account take over fraud". Do not check the "computer intrusion" box.[4]
- If the account take over involves a wire transfer, then in addition to selecting the "other" box with the notation "account take over fraud", the "wire transfer" box should also be checked on the current SAR form.
- If the account take over involves an ACH transfer, the financial institution should check the "other" box and note "account take over fraud – ACH".
- If the account take over involved other delivery channels such as Telephone Banking or other fraud activities such as social engineering, the financial institution should check the "other" box and note "account take over fraud' and include a short description of the additional information.
- Other relevant boxes may be checked if appropriate (i.e. terrorist financing, identity theft, etc.).
- In addition, the narrative section of the SAR should contain the term "account take over fraud" and provide a detailed description of the violation of law or suspicious activity including any additional delivery channels used in the fraud and any additional fraudulent activities used to perpetrate the fraud.

Financial institutions are also encouraged to fax a copy of the SAR to law enforcement. To determine local law enforcement contacts in your area, see the law enforcement directory under the contact directory within the FS-ISAC portal.

### 2.6.4. Timing of a SAR Filing

A financial institution is required to file a SAR in accordance with the instructions, no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a suspicious activity report. If no

[4] FinCEN defines "computer intrusion" as gaining access to a computer system of a financial institution to: (a) remove, steal, procure or otherwise affect funds of the institution or institutions customers; (b) remove, steal, procure or otherwise affect critical information of the institution including customer account information; (c) damage, disable or otherwise affect critical systems of the institutions. Computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information. It also does not apply to the typical corporate account take over that involves gaining access to a customer computer system through the use of malware that does not affect the computer system of a financial institution.

suspect was identified, on the date of detection of the incident requiring the filing, a financial institution may delay filing a suspicious activity report for an additional 30 calendar days to identify a suspect.

In no case shall reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction.

Supplemental SARs should be filed every 90 days if:

- A suspect is added or deleted.
- The risk amount to the bank increases.
- The pattern of fraudulent activity continues for a period of time.

## 2.7. Post Mortem Activities

Post mortem activities can be time consuming; however, if the breach is large and the investigation uncovered uncontrollable events or errors, a post mortem is recommended. These activities can be important to identify new fraud trends, determine if your current detection strategy is effective, and identify new processes or changes needed in the current response strategy.

- As part of your monitoring program, identify a central repository where information on alerts are generated, actions taken are tracked, and intelligence associated with the events can be analyzed.
- So that your teams can continue to learn and adapt, ensure new account take over events are being compared against historical events to help identify important trends and issues requiring further attention. Items to address with this procedure include:
    - How did the compromise occur (or how were they infected)?
    - Was it internal or external?
    - Was the event targeted or opportunistic?
    - What mechanism(s) were used to gain access to the account?
    - If malware was involved, what's the nature of the malware?
    - Are other organizations seeing similar activity?
    - What was the point of compromise?
    - How was the event detected? (by the fraud detection system or by the customer)
    - Were the actions taken effective? If not, what improvements can be made?

- Are there additional controls which need to be recommended to the customer or across the customer base?

## *2.8. Conclusion*

The strategy used by a financial institution to respond to account take over events should be tailored to the products and services that are offered while considering the types of fraud cases that have been experienced by the organization. Depending on the risks involved, several response methods may need to be implemented to ensure proper mitigation of those risks.

# Appendix 1- Recommendations for Reporting an Account Take Over via SARs

To ensure a consistent reporting process for account take over via a SAR:

- Check the "other" box with a notation "account take over fraud". Do not check the "computer intrusion" box.[5]
- If the account take over involves a wire transfer, then in addition to selecting the "other" box with the notation "account take over fraud", the "wire transfer" box should also be checked on the current SAR form.
- If the account take over involves an ACH transfer, the financial institution should check the "other" box and note "account take over fraud – ACH".
- If the account take over involved other delivery channels such as Telephone Banking or other fraud activities such as social engineering, the financial institution should check the "other" box and note "account take over fraud' and include a short description of the additional information.
- Other relevant boxes may be checked if appropriate (i.e. terrorist financing, identity theft, etc.).
- In addition, the narrative section of the SAR should contain the term "account take over fraud" and provide a detailed description of the violation of law or suspicious activity including any additional delivery channels used in the fraud and any additional fraudulent activities used to perpetrate the fraud.

Financial institutions are also encouraged to fax a copy of the SAR to law enforcement. To determine local law enforcement contacts in your area, see the law enforcement directory under the contact directory within the FS-ISAC portal.

[5] FinCEN defines "computer intrusion" as gaining access to a computer system of a financial institution to: (a) remove, steal, procure or otherwise affect funds of the institution or institutions customers; (b) remove, steal, procure or otherwise affect critical information of the institution including customer account information; (c) damage, disable or otherwise affect critical systems of the institutions. Computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or customer financial or other critical information. It also does not apply to the typical corporate account take over that involves gaining access to a customer computer system through the use of malware that does not affect the computer system of a financial institution.