SNBT HOME

Business Incident Response Checklist

Remember the key to increasing the likelihood that you can recover all or some of your funds is to complete the below steps IMMEDIATELY

Alert employees of confirmed or suspected corporate account takeover

- ☐ Notify and update applicable parties.
- ☐ Employees should have predetermined responsibilities, for example:
  - — **Management:** Oversee and coordinate process
  - — **IT Department**(may be outsourced): Identify and mitigate further attacks
  - — **Bookkeeping/ACH Officer**: Work with financial institution on recovery
  - — **Corporate Security**: Contact law enforcement
  - — **Public Relations**: Work on press release if needed
  - — **Legal Counsel** (internal or external): Consider and coordinate legal issues

Notify your financial institution

- ☐ Make sure all online banking functions are disabled or suspended.
- ☐ Determine a plan to handle legitimate online banking account functions needed during the investigation period with your financial Institution. What is your plan?

  _____
- ☐ Review your recent deposit account activity for authenticity.
- ☐ Close effected deposit account(s) and open replacement account(s). (*if necessary*)

  List closed account number(s): _____

  List new account number(s): _____

Gather and document information on the incident

- ☐ How do you know about the issue? Who reported it? _____

  _____
- ☐ What is the User ID used in the incident? _____
- ☐ Was it shared?_____
- ☐ How does the user log in? *(token, password, biometrics)*_____
- ☐ Did the user notice anything unusual during the log in process? *(picture/phrase different, slow response, website unavailable, redirected)*_____

  _____
- ☐ What (if any) additional authentication is required upon transmission of funds? (*fax transmittal, token, call back)* _____
- ☐ Have you confirmed that this incident is in fact fraudulent?_____

- ☐ How and when did you confirm this?_____

Gather details on the fraudulent transactions and attempt to stop transfers of funds *(work with your financial institution)*

- ☐ Date(s) of incident(s): _____
- ☐ Type of transaction involved: _____
- ☐ **Request assistance from your Financial Institution to stop pending transfers and initiate reversal file(s) as necessary.**
- ☐ Dollar amount, ABA, and Account numbers involved: _____

_____

_____

Attempt to recover lost funds and plan for recourse *(if not caught prior to settlement date)*

- ☐ Ask for assistance of your financial institution to reach out to the other financial institutions involved in attempt to recover any unauthorized fund transfers.
- ☐ Note funds you are able to recover:_____

_____

- ☐ Note funds you are not able to recover:_____

_____

- ☐ Contact your insurance company and determine what coverage you have on any loss. Notes: _____
- ☐ Have your public relations contact prepare a press release (if applicable).
- ☐ Contact local law enforcement and obtain a copy of the police report. Notes: _____

_____

- ☐ File a complaint with the Internet Crime Compliant Center at: **www.ic3.gov**
- ☐ For substantial losses contact your local:
  - FBI field office: **www.fbi.gov/contact-us/field/field-offices**
  - Secret Service field office: **www.secretservice.gov/field_offices.shtml**
  - Secret Service Electronic Crime Task Force: **www.secretservice.gov/ectf.shtml**

Identify vulnerability and begin a plan to remedy

- ☐ Does the compromised user access the online banking account via more than one computer station or by remote access?_____

Business Incident Response Checklist

- ☐ Is the compromised computer connected to the network?_____
- ☐ Has the computer(s) been checked for malware and viruses by up-to-date anti-virus software? _____Who conducted the scan? _____
- ☐ When was the last time the user legitimately logged into the online banking account? (*This date may help determine the date of infection)*_____
- ☐ How did the computer become infected with malware?
  - — User opened Infected email attachment
  - — User clicked on infected website link within email
  - — User clicked on infected document, picture, or video in legitimate website (social networking site).
  - — Other: _____
- ☐ Is this user name and password the same for other sites? _____
  If yes, the user should change this information immediately.
- ☐ User should delete temporary Internet files and cookies to avoid fraudulent access to "saved" user names and passwords on other sites.
- ☐ Once you have identified the extent of the vulnerability, remove the malware. Keep in mind that in some cases the computer(s) may need to be rebuilt or replaced.
- ☐ Confirm what your financial institution requires to verify that the vulnerability has been remedied. *(internal investigation or third party analysis)*
- ☐ Provide your financial institution with written documentation of how the breach occurred and what has been done to remedy the breach. Keep this documentation in your records.
- ☐ Once you can prove either that the malware has been removed and that the compromised computer is clean, or that the compromised computer has been rebuilt or replaced, ask your financial institution to reinstate access to online banking account & reactivate any other suspended services.

Prevent future instances of Corporate Account Takeover

- ☐ Utilize Best Practices for Businesses to develop policies and procedures to mitigate future instances of corporate account takeover.
- ☐ Hold an "After the Event" meeting with key staff members and financial institution representative(s) to discuss how to improve mitigation techniques.