



# TEXAS BANKERS ELECTRONIC CRIMES TASK FORCE

---



## Bulletin 2012-3

April 5, 2012

*The following is a recent action or issuance to be considered in the risk management practices for reducing the risks of Corporate Account Takeovers through the Protect, Detect, and Respond framework.*

## Reporting Account Takeover Activity to FinCEN

---

The Financial Crimes Enforcement Network (FinCEN) issued [FinCEN Advisory 2011-A016](#) on December 19, 2011 to assist financial institutions with identifying account takeover activity and reporting the activity through the filing of Suspicious Activity Reports (SARs). The FinCEN Advisory recommends that financial institutions use the term "account takeover fraud" in the narrative section of the SAR and provide a detailed description of the activity.

To further enhance the usefulness of the SAR filing, financial institutions may want to consider the following examples when completing the Suspicious Activity Information section:

- Check the "other" box and note "account takeover fraud" in the space provided.
  - Depending upon the activity, also check:
    - "Computer Intrusion," if an intrusion or compromise of any of the bank's computers is involved.
    - "Wire Transfer Fraud", if a wire transfer is involved.
    - "Identity Theft", if the account takeover involved unauthorized access to PINs, account numbers, and other identifying information.
    - Any additional boxes, if appropriate (e.g. "terrorist financing").
- If other delivery channels such as telephone banking or fraudulent activities such as social engineering are involved, include a short description in the space provided by the "other" box along with the description "account takeover fraud".

- If an ACH transfer is involved, note "account takeover fraud – ACH" next to the "other" box.

**Recommended Action:**

Notify the BSA Compliance Officer when account takeover activity is suspected to ensure that SARs related to account takeover fraud are reported.