

Bank Secrecy Act (BSA)

BSA-AML-CIP-OFAC for I.S. & I.T.

What is the BSA?

- The Bank Secrecy Act (BSA) requires all financial institutions, casinos, and certain other businesses to:
 - Monitor customer behavior
 - File reports on transactions that meet certain dollar amounts
 - Maintain records of certain transactions
 - The Currency Transaction Report (CTR), which records cash transactions that exceed \$10,000.
 - The Suspicious Activity Report (SAR), which records any known or suspected federal violation of federal law.
- The BSA aids law enforcement by uncovering criminal activities such as money laundering, drug trafficking, tax fraud, and possible terrorist financing.

USA Patriot Act

- After September 11th, President Bush signed into law the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act**
- Provides additional tools to prevent, detect, and prosecute international money laundering and the financing of terrorism.

Office of Foreign Assets Control

- **OFAC is part of the US Treasury Dept and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries, terrorists, and international narcotics traffickers**
- **Parties subject to the OFAC sanctions are:**
 - Specially Designated Nationals
 - Specially Designated Terrorists
 - Specially Designated Narcotics Traffickers
 - Blocked Persons
 - Blocked Vessels
- **OFAC laws require banks to identify any transactions and property subject to the economic sanctions**
- **Once identified, the asset must be blocked or the transaction may be rejected**

What Is Money Laundering?

- Money Laundering is when illegal money is brought into the mainstream circulation.
- Launderers hide the source of these illegal funds by making a series of intricate transactions. The true source of the money is “washed away.”



Suspicious Activity Report (SAR)

- A Suspicious Activity Report (SAR) must be filed on any known or suspected federal violation of law. Suspicious activity requires reporting if it involves at least \$5,000 aggregate, and the institution knows or suspects that (for example):
 - The funds are derived from illegal activities
 - The funds are part of a plan to violate or evade any federal law or regulation
 - The transaction is designed to evade other reporting requirements
 - The transaction is not the sort in which the particular customer would normally be expected to engage, and the institution knows of no reasonable explanation for the transaction.



Something Ain't Right



- The first question you ask is if the activity is reasonable for that customer. If not, then that rises to the level of suspicious activity.
- Whether the action is ultimately a fraud is up to law enforcement to decide.
- Think Ghostbusters!

*“when there’s something strange in your neighborhood, who ya gonna call?
If there's something weird and it don't look good, who you gonna call?”*

Detecting Suspicious Transactions

■ Unusual Characteristics or Activities

- A dormant account containing a minimal sum suddenly receives a deposit or series of deposits followed by daily cash withdrawals that continue until the transferred sum has been removed.

■ Notification or Discovery of Counterfeit Checks

■ Transactions Linked to Locations of Concern or Initiated by Persons Whose Names Appear on the OFAC List

■ Certain Funds / Wire Transfer Activities

- Sending or receiving frequent or large volumes of wire transfers to and from offshore institutions.
- Wire transfers ordered in small amounts in an apparent effort to avoid triggering identification or reporting requirements.

■ Certain Bank Employees

- An employee whose lavish lifestyle cannot be supported by his or her salary.
- An employee who conducts transactions on their own behalf
- An employee who is associated with mysterious disappearances or unexplained shortages of significant amounts of Bank funds.

If you believe your customer may be conducting Suspicious Activity ... Notify your supervisor immediately.

Do Not attempt to have a conversation with the customer before discussing with the BSA Officer.

What is Structuring?

- Structuring is a common tactic used to launder money, specifically to place funds into the financial systems.
- A transaction is structured by **breaking down a single sum of currency of more than \$10,000 into smaller currency transactions**. The transaction can consist of either deposits or withdrawals in amounts under \$10,000.
- A person can act alone, or on behalf of another individual or business, in order to cause an institution to fail to file a CTR.
- **Structuring Examples:**
 - After learning that a CTR will be filed, an individual attempts to reduce the transaction to fall below the reporting requirement of more than \$10,000.
 - An individual conducts multiple transactions over the course of several days in amounts less than \$10,000. (e.g. \$9,900 - \$9,500 - \$9,950)

Other Types of Reportable Activity

- Bribery
- Check Fraud
- Check Kiting
- Computer Intrusion
- Counterfeit Check
- Counterfeit Credit/Debit Card
- Credit/Debit Card Fraud
- Embezzlement
- Mortgage Fraud
- False Statement
- Loan Fraud
- Misuse of Position
- Mysterious Disappearance
- Wire Transfer Fraud
- Tax Evasion
- Terrorist Financing
- Identity Theft

But not our customers!

- In 2009, ABC BANK was contacted ## times by various Law Enforcement Agencies regarding ## different customers:
 - List agencies here
- We've seized over \$\$\$\$\$\$ related to illegal activity!

Penalties for Noncompliance

- **Violations of BSA requirements may hold civil and / or criminal penalties, such as:**
 - Civil penalties of \$1000 per day for each day of noncompliance.
 - A penalty of \$500 per violation of the recordkeeping requirements of the BSA.
 - Willful violations may cause civil penalties in an amount equivalent to that of the transaction or \$25,000, whichever is greater.
 - If a required CTR is not filed within 15 days, a \$10,000-per-day civil penalty may be imposed until it is filed.
 - **Continued noncompliance can result in the issuance of a “Cease & Desist” order from the FDIC.**
- Any individual who willfully violates the structuring provisions may be **fined \$250,000 and/or imprisoned for five (5) years.**
- Any individual who willfully violates the structuring provisions while violating another federal law, may be **fined \$500,000 or imprisoned for ten (10) years.**

Penalties for Noncompliance

- It is extremely important for all employees to know that it is not necessarily the bank that will suffer the penalty for non-compliance, but it could actually be the employee paying the fine and going to jail.
- Please do not compromise your position at the bank by ignoring these regulations.



C'mon – no one has been finedRight?

- **4/20/09 - Doha Bank New York**
 - \$10 Million Civil Money Penalty (CMP)
- **01/02/09 - E*Trade**
 - CMP \$1 Million.
- **10/16/08 - Sanderson State Bank**
 - Cease & Desist (CD)
 - Note: This bank was closed by Texas Department of Banking on 12/12/08
- **07/30/08 - E*Trade**
 - CD & CMP \$1 Million.
- **9/14/2007 - Union Bank of California**
 - CMP \$10 million
 - Forfeiture. \$21.6 million
- **8/3/2007 - American Express**
 - C&D order
 - CMP \$20 million (bank)
 - CMP \$5 million (company)
 - Forfeiture. \$55 million (bank)

BANKS

- 10/26/2009 - Family B&T - Forfeiture
- 08/05/2009 - First Standard Bank - C&D
- 08/04/2009 - Heritage Bank of North Florida - C&D
- 04/20/2009 - Doha Bank - CMP
- 04/02/2009 - Rocky Mountain B&T - C&D
- 02/24/2009 - Bank of Westminster - C&D
- 02/17/2009 - Directors of Sykesville FSA - CMPs
- 02/12/2009 - Upstate National Bank - C&D
- 02/12/2009 - University Bank - C&D
- 01/29/2009 - First Vietnamese American Bank - C&D
- 01/02/2009 - E*Trade Clearing LLC et al - Fine
- 12/03/2008 - West Suburban Bank - C&D
- 11/13/2008 - Mountain Commerce Bank - C&D
- 11/07/2008 - Dresdner Bank AG - C&D
- 11/03/2008 - Blue Ridge Savings Bank, Inc. - C&D
- 10/27/2008 - Polk County Bank - C&D
- 10/24/2008 - Eastern National Bank - CMP
- 10/17/2008 - Fort Davis State Bank - C&D
- 10/16/2008 - Sanderson State Bank - C&D
- 10/07/2008 - Omni National Bank - C&D
- 10/02/2008 - Kenney Bank and Trust - C&D
- 10/02/2008 - The Bank of Harlan - C&D
- 09/25/2008 - First Asian Bank - C&D
- 09/15/2008 - Citizens Community Bank - C&D
- 09/09/2008 - Intercredit Bank, N.A. - C&D
- 08/27/2008 - Mizrahi Tefahot Bank, Ltd. - C&D
- 08/21/2008 - Chestatee State Bank - C&D
- 07/30/2008 - E*Trade Clearing LLC et al - C&D & CMP
- 07/09/2008 - T Bank, N.A. - C&D
- 06/04/2008 - Eastern National Bank - C&D
- 04/30/2008 - Sun Security Bank - C&D
- 04/22/2008 - United Bank for Africa, PLC - CMP
- 04/14/2008 - EI Noa Noa - CMP
- 03/14/2008 - Independence Bank - C&D
- 03/10/2008 - First Regional Bank - C&D
- 02/29/2008 - United Bank for Africa, PLC - C&D
- 02/26/2008 - Wallis State Bank - C&D
- 02/19/2008 - Doral Bank - C&D
- 01/24/2008 - Sigue Corporation and Sigue, LLC - CMP
- 12/19/2007 - The State Bank of Lebo - C&D
- 12/03/2007 - The Citizens Bank of Weir, Kansas - C&D
- 10/30/2007 - Pan American Bank - C&D
- 10/18/2007 - Pan Pacific Bank - C&D

Family Bank and Trust Company (FBTC), an FDIC-insured non-member bank located in Palos Hills, Illinois, entered into a plea-bargain agreement announced on 10/26/09 by the U.S. Attorney for the Northern District of Illinois. The bank agreed to plead guilty to federal criminal charges that it conspired with its former CEO and others to fail to file multiple CTRs involving deposits totaling more than \$800,000. In its plea agreement, the bank agreed with the government to ask a judge to impose probation and a forfeiture of \$800,000.

FBTC was closely held by its former president, Marvin Siensa, now deceased. The charges allege that Siensa and others caused the bank to fail to file CTRs on multiple cash deposits, and to use nominee accounts to disguise the nature of the deposits, which were largely the proceeds of illegal activity, allegedly international trafficking in pseudoephedrine, a key ingredient in the manufacture of methamphetamine.

Remote Deposit Capture

Risk Factors

- RDC may expose Banks to various risks, including money laundering, fraud, and compromised transmission of financial data.
 - Duplicate Deposits and /or Items
 - Forged Endorsements
 - Counterfeit Items
 - Alterations
- Inadequate controls could result in the transmission of fraudulent monetary instruments, exposing the Bank to financial and reputational risks.
- Because RDC equipment is located outside of Bank facilities, data and hardware security issues may increase.

ACH (Automated Clearing House)

- The BSA requires banks to monitor and identify unusual activity, including ACH transactions.
- ACH transactions can be used in the layering and integration stages of money laundering. Detecting unusual activity in the layering and integration stages can be a difficult task, because ACH may be used to legitimize frequent and recurring transactions. Banks should consider the layering and integration stages of money laundering when evaluating or assessing the ACH transaction risks of a particular customer.

Your Responsibility

- The IS/IT staff is required to know their customers and employees.
- Some activity may initially appear suspicious but, with a reasonable explanation, may be determined not suspicious.
- Be aware of the Banks's designated Medium and High Risk customers
- Report any unusual/suspicious activity to the BSA Officer.

The Fine Print

- It is the policy of the Bank that all requirements of the Bank Secrecy Act are to be complied with. Willful failure to do so will result in immediate suspension, without pay, or termination.
- Employees who observe incidents of suspected violations, or failure to report transactions involving customers or fellow employees, are obligated to report such incidents to Risk Management or the Bank Secrecy Act (BSA) Officer. If the employee does not do so, they could be subject to disciplinary action, up to and including termination, and criminal prosecution.
- No employee shall be disciplined for properly reporting suspicious activity.

| 1. *WHO (Suspect Name) | *Tax ID/EIN | *Birth Date | *Profession | *Physical Address | *DL/ID # | *Phone # |
|-------------------------------|-------------|-------------|-------------|-------------------|----------|----------|
| | | | | | | |
| | | | | | | |

2. ***What category does this report belong in? * indicates "most common"**

| | | | | | | |
|---|--|--|--|---|---|-------------------------------------|
| <input type="checkbox"/> Computer Intrusion | <input type="checkbox"/> Credit Card Fraud | <input type="checkbox"/> * Kiting | <input type="checkbox"/> * Lottery Scheme | <input type="checkbox"/> Mysterious Disappearance | <input type="checkbox"/> * Tax Evasion | <input type="checkbox"/> Wire Fraud |
| <input type="checkbox"/> * Counterfeit Check | <input type="checkbox"/> ID Theft | <input type="checkbox"/> Loan Fraud | <input type="checkbox"/> * Money Laundering | <input type="checkbox"/> * Structuring | <input type="checkbox"/> Terrorist Activity | <input type="checkbox"/> Other |

3. **Account #'s Involved & Date Opened:**

4. *** Explain The Activity In Detail (WHAT and HOW):**

5. *** WHERE Did The Activity Take Place? (Include All Locations Involved):**

6. *** Explain WHY You Think This Activity Is Suspicious. (For Help Please Refer To The Information Provided On This Form).**

7. *** WHEN Did The Activity Occur?:**

From: Through:

8. **List Any Other Individuals Involved:**

9. *** Branch Preparing Report:**

10. *** Report Prepared By:**

Date:

11. *** Approved By:**

Date:

(print name)

(approval signature)

12. *** Attach a copy of the signature card(s).**

<http://www.bankersonline.com/tool>

13. *** Attach any supporting documentation.**