SKIPO JEOPARDY STUDY GUIDE

SUSPICIOUS ACTIVITY

Banks and other financial institutions are required to use the SAR form to notify law enforcement agencies when they detect a known or suspected violation of federal law, including a violation of the Bank Secrecy Act or a suspicious transaction related to money laundering activity. Suspicious Activity may include practices such as large cash exchanges, wires into an account followed by transfers out, and structuring of cash transactions to avoid CTR reporting. In addition, suspicious activity and money laundering may be accomplished by lesser known methods such as purchasing a Time Deposit using "dirty" cash proceeds, and using that money to secure a loan, and paying down a large problem loan with cash. All Bank employees must be aware of what constitutes suspicious activity, and report all such activity to xxxxxxx, BSA Officer.

KNOW YOUR CUSTOMER

The "Know Your Customer" policy is probably the cornerstone of the Bank Secrecy Act. SSB has implemented the BSA recommendations dealing with customer identification and record-keeping, such as asking for driver's licenses, State ID Cards, Resident Alien Cards, utility bills, and Tax Identification numbers when establishing a relationship with a client. When establishing business relationships, employees should request such items as articles of incorporation, partnership agreements, proof of prior banking relationships, the type of business activity, the business' address and the business' Employer Identification Number. Once the relationship is established, Thank-You letters, site visits, and periodic transaction monitoring are tools the Bank uses to ensure the account is legitimate. If an individual cannot establish their identity to the satisfaction of the Bank, the Bank may refuse to open the account. If the activity in an established account is questionable the Bank may close the account, notify Security and Regulatory Management, and send the client a letter explaining our decision.

INFORMATION SECURITY

Sandy Spring continually updates and improves our security standards and procedures to help us protect against anyone gaining unauthorized access to our client's confidential information and to prevent fraud. Our Information Security Officer, xxxxxx, has established a bank-wide policy that mandates security measures both in physical security and technological security. Some of the physical devices we use include shredding of confidential information, use of key pads, locked doors and security cameras to protect our physical premises, and the use of locked drawers, vaults and file cabinets to protect

and store our client's information. To protect our computer data, such practices as downloading unauthorized software, accessing porn sites, and the use of AOL instant messenger are prohibited practices for all bank employees.

PRIVACY/ IDENTITY THEFT

Effective last year, all financial service providers such as Banks were required to abide by the rules set forth in title V of the Gramm-Leach-Bliley Act to protect all customer's non-public personal information. This law, implemented by Federal Reserve Regulation P, made it mandatory for each Bank to provide a notice outlining our information sharing practices to each customer (defined as consumers who have an ongoing relationship with the bank). These notices must be given when an account is opened, a loan is closed, and must be mailed annually to every customer. The law allows banks to share non-public personal information under certain limited exceptions with entities such as Equifax, Deluxe, ChexSystems, and Metavante who process customer transactions. Banks that share information outside of these exceptions must allow customers the opportunity to "opt-out" of such sharing. Sandy Spring does not share customer information outside the exceptions, so it is not necessary for our clients to "opt-out" with us.

This same law mandates that Banks protect their customers from identity theft, by ensuring that information regarding a customer's account is given only to that customer or someone legally authorized to act on the customer's behalf. Identity theft is a criminal activity where an individual wrongly obtains and uses another person's personal data without their knowledge and consent to commit fraud. The bank can prevent identity theft by asking the right questions to identify a caller, or asking for proper ID when an unknown person is requesting account information.

OFAC

The Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury administers and enforces economic and trade sanctions against targeted foreign countries, terrorism sponsoring organizations and international narcotics traffickers based on U.S. foreign policy and national security goals. OFAC acts under presidential wartime and national emergency powers, as well as authority granted by specific legislation. Under these laws, financial institutions, securities firms, and insurance companies are obligated to block or "freeze"' property and payment of any funds transfers or transactions and to report all blockings to OFAC within ten days of occurrence. Any institution in non-compliance is open to adverse publicity, fines, and even criminal penalties. Metavante "scrubs" our client database nightly for new accounts, and because OFAC frequently adds and deletes names and countries, Metavante performs monthly "scrubs" on the entire database for any new names or countries. Countries such as Iran, Iraq, and Cuba, and people such as Osama Bin Laden and other known terrorists and narcotics traffickers are found on the OFAC list. As the OFAC Officer, xxxxx is responsible for OFAC compliance Bank-wide.

FYI: The Bank's Privacy Policy, Information Security Policy, BSA Policy, Know Your Customer Policy, and Identity Theft Policy are available on the SSB Intranet. The OFAC list can be accessed at http://www.treas.gov/ofac/