SOUTH DAKOTA
Division of Banking

1601 N. Harrison Ave, Suite 1
Pierre, SD 57501
Phone (605) 773-3421
Fax (866) 326-7504

Bank Secrecy Act Guidance

On October 26, 2001, the USA PATRIOT Act (Patriot Act) became effective. The Patriot Act brought significant amendments and additions to the customer identification and anti-money laundering provisions of the Bank Secrecy Act (BSA). The United States Department of Treasury (Treasury) rules implementing BSA are codified at Title 31 Code of Federal Regulation (CFR) Chapter X entitled "Financial Recordkeeping and Reporting of Currency and Foreign Transactions." Chapter X Section 1010.100 defines a financial institution to include a commercial bank or trust company organized under the laws of any state or of the United States. In short, all South Dakota chartered trust companies must develop and implement policies and procedures to ensure compliance with BSA reporting requirements. The South Dakota Division of Banking (Division) performs a BSA review in conjunction with each trust company's regularly scheduled examination. Trust company management is strongly encouraged to consult with legal counsel or others with knowledge and expertise in the field in developing a program for BSA compliance that is specific to each trust company's respective business plan.

The following guidance is not all inclusive, but provides trust company management with fundamental BSA provisions:

Anti-Money Laundering Program (Exclusionary Language)

Section 1010.210 requires financial institutions to establish an Anti-Money Laundering (AML) Program. However, Section 1010.205 exempts non-federally regulated trust companies from the requirements in Title 31 USC 5318(h)(1) concerning the establishment of an AML Program. Specifically exempted are the development of internal policies, procedures, and controls; the designation of a compliance officer; an ongoing employee training program; and an independent audit function for testing purposes. Although non-federally regulated trust companies are exempted from many of the requirements that regulated banks must comply with, it would be beneficial for trust companies to complete a risk assessment of their products and services, customer base, and geographic location(s) to assist in identifying any potential areas that may present a higher level of risk for money laundering activity. Refer to the Financial Crimes Enforcement Network (FinCEN) website for risk assessment guidance. The FinCEN website should be used as a resource for trust companies to review statutes and administrative rulings, access forms, obtain definitions, review FAQ's, and review federal register notices.

Customer Identification Program

Section 1010.220 requires financial institutions, including trust companies, to establish a Customer Identification Program (CIP). Section 1020.220 provides specific guidance for creating and maintaining an adequate CIP. The CIP covers accounts established to provide custodial and trust services. Generally, a trust company must implement a written CIP commensurate with its size and complexity. The intent of the regulation, at a minimum, is to require financial institutions to implement reasonable procedures to verify the identity of any person seeking to open an account, to the extent reasonable and practicable; maintain records of the information used to verify the person's identity; and determine whether the customer appears on any list of known or suspected terrorists or terrorist organizations issued by any Federal government agency. To date, no Federal government agency has provided the Division with a list of known or suspected terrorists or terrorist

organizations. Financial institutions will be notified once a list is designated for the purposes of this regulation. In the meantime, there are no interim requirements for checking any lists for CIP compliance.

Office of Foreign Assets Control Reporting

Financial institutions should be aware that Office of Foreign Assets Control (OFAC) review provisions are separate and distinct from the CIP provisions requiring financial institutions to compare new accounts against government lists of known or suspected terrorists or terrorist organizations. The OFAC review identifies countries, entities, and individuals that pose a threat to the national security, foreign policy, or economy of the United States. Every financial institution is required to periodically review OFAC-generated lists to determine and report any "hits." While not required by specific regulation, financial institutions should establish and maintain an effective, written OFAC compliance program commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify higher-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate an employee responsible for OFAC compliance, and ensure training for appropriate personnel in all relevant areas of the institution. The OFAC compliance program should be commensurate with the financial institution's respective risk profile.

Financial Crimes Enforcement Network Section 314(a) Reporting

Financial institutions should also be aware that their responsibilities to share information with FinCEN are separate and distinct from CIP and OFAC provisions. FinCEN issues Section 314(a) notices, approximately every two weeks. When these notices (which identify individuals and entities suspected of illegal activities) are received, financial institutions are required to compare their customer list with the list of businesses and individuals on the 314(a) notice to determine and report any positive matches. The requests contain subject and business names, addresses, and as much identifying data as possible to assist the financial industry in searching their records. The financial institutions must query their records for data matches, including accounts maintained by the named subject during the preceding twelve months and transactions conducted within the last six months. Financial institutions have two weeks from the posting date of the request to respond with any positive matches. If the search does not uncover any matching of accounts or transactions, the financial institution is instructed not to reply to the 314(a) request.

Regulatory authorities impose FinCEN review and reporting provisions on the institutions they supervise. Beginning in 2015, the Division is requiring all South Dakota-chartered public trust companies to comply with FinCEN reporting provisions. In order to obtain access to the 314(a) Secure Information Sharing System (SISS), each public trust company is required to submit to the Division the following information:

- Point of contact name;
- Point of contact email address and phone number;
- Trust company tax identification number; and,
- Trust company fax number.

The Division will forward the information to FinCEN for processing. The designated point of contact will then receive a notification from FinCEN whenever new 314(a) case information has been posted on the SISS. After receiving FinCEN notification, each public trust company will register their user name (which is their full email address), and will get a temporary password to access the system.

Currency Transaction Reporting

Section 1010.310 requires financial institutions, including trust companies, to report currency transactions involving amounts greater than $10,000, subject to certain exceptions. It is acknowledged that transactions involving trust and other fiduciary accounts rarely involve currency, but if such a transaction occurs and the amount is greater than $10,000, then the trust company must file a Currency Transaction Report with the Internal Revenue Service within 15 days of the transaction.

Suspicious Activity Reporting

Section 1010.320 requires financial institutions, including trust companies, to file a Suspicious Activity Report (SAR) with FinCEN for transactions involving $5,000 or more in funds and assets if the institution knows, suspects, or has reason to suspect that:

- The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- The transaction is designed to evade any requirements of this part or of any other regulations promulgated under BSA regulations; or,
- The transaction has no business or apparent lawful purpose or is not the sort in which the particular customer would normally be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Foreign Financial Account Reporting

Section 1010.350 requires financial institutions, including trust companies, to file a Report of Foreign Bank and Financial Accounts (TD-F 90-22.1), or any successor forms. In general, each United States person having a financial interest in, or signature or other authority over, a bank, securities, or other financial account in a foreign country shall report such relationship to the Commissioner of Internal Revenue for each year in which such relationship exists.