SOUTH DAKOTA
Division of Banking

1714 Lincoln Avenue, Suite 2
Pierre, SD 57501
Phone (605) 773-3421
Fax (866) 326-7504

Anti-Money Laundering and Countering the Financing of Terrorism Guidance

On October 26, 2001, the USA PATRIOT Act became effective, bringing significant amendments and additions to the customer identification and Anti-Money Laundering (AML) provisions of the Bank Secrecy Act (BSA). The U.S. Department of the Treasury rules implementing BSA are codified at Title 31 Code of Federal Regulations (CFR) Chapter X entitled "Financial Crimes Enforcement Network, Department of the Treasury." 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 U.S.

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 an AML/Countering the Financing of Terrorism (CFT) 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 AML/CFT 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 information pertaining to AML/CFT provisions and requirements. Management should refer to the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual for additional guidance.

<u>Anti-Money Laundering Program</u>

Section 1010.210 requires financial institutions, including trust companies, to establish an AML program designed to guard against using the trust company to facilitate money laundering or terrorist financing. On September 15, 2020, the Financial Crimes Enforcement Network (FinCEN) issued a final rule that amended Section 1010.210 to include state-chartered non-depository trust companies within the definition of a "bank" for AML purposes. Additionally, FinCEN amended Section 1020.100 and removed Section 1010.205, which effectively ended all prior AML exemptions for persons or entities subject to supervision by state banking authorities. As such, all state-chartered non-depository trust companies are required to include the following components in their AML Programs:

- Development of internal policies, procedures, and controls.
- The designation of a compliance officer.
- An ongoing employee training program.
- An independent audit function for testing purposes (completed every 12 to 18 months based on the institution's risk profile).
- Appropriate risk-based procedures for conducting ongoing customer due diligence, to include, but not be limited to:
  a. Understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and,
  b. Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

FinCEN's final rule permits each institution lacking a federal functional regulator to take a risk-based approach to tailor its AML program to suit its own size, needs, and operational risks. Therefore, all South Dakota-chartered trust companies are required to complete annual risk assessments 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. The risk assessment should be reviewed, approved, and documented in Board meeting minutes. Refer to the FinCEN website or the FFIEC BSA/AML Examination Manual for risk assessment and other AML guidance. The FinCEN website should be used as a resource for trust companies to review statutes and administrative rulings, access forms, obtain definitions, review FAQs, 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 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 if 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.

Customer Due Diligence – Beneficial Ownership Rule

Section 1010.230 requires financial institutions, including trust companies, to establish and maintain written procedures that are reasonably designed to identify and verify the beneficial owners of legal entity customers and to include such procedures in their AML Program required under 31 U.S.C. 5318(h) and its implementing regulations. The Beneficial Ownership Rule was applied to state-chartered non-depository trust companies by FinCEN's final rule issued on September 15, 2020. Effective November 16, 2020, all South Dakota-chartered trust companies were required to begin the process of identifying and verifying the beneficial owners of legal entity customers with full compliance by March 15, 2021. Refer to the Division's Customer Identification Guidance and FinCEN's website for Beneficial Ownership Rule guidance.

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. OFAC review provisions require 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 U.S. 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 in the Section 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 financial institutions 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 Section 314(a) request.

Financial Institutions must work directly with FinCEN to add, remove, or modify an existing Section 314(a) Point-of-Contact. Information regarding financial institution access is available at the following website: https://www.fincen.gov/resources/financial-institutions.

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 FinCEN within 15 days of the transaction; therefore, trust companies must have written policies and procedures in place in the event such a transaction occurs.

Suspicious Activity Reporting

Section 1010.320 requires banks, including trust companies, to file a Suspicious Activity Report (SAR) with FinCEN for transactions if the bank/trust company **knows, suspects, or has reason to suspect** that the transaction involves:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank/trust company (or affiliate) and aggregating $5,000 or more, if the bank/trust company (or affiliate) knows, suspects, or has reason to suspect that the transaction:
    - May involve potential money laundering or other illegal activity (e.g., terrorism financing).
    - Is designed to evade the BSA or its implementing regulations.

- Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank/trust company knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A bank/trust company is required to file a SAR no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If no suspect was identified on the date of the detection of the incident requiring the filing, a bank/trust company may delay filing a SAR for an additional 30 calendar days to identify a suspect. In no case shall reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction. A bank/trust company shall maintain a copy of any SAR filed and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR. A SAR, and any information that would reveal the existence of a SAR, are confidential and shall not be disclosed except as authorized at 31 C.F.R., Chapter X, Section 1020.320(e)(1).

Policies, procedures, and monitoring systems are an integral part of the SAR program and process. All banks/trust companies must ensure that there are adequate systems in place to identify, monitor, and report any potential suspicious activities. The sophistication of monitoring systems should be dictated by the bank/trust company's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographic locations. Written guidance must reflect the following five components of an effective monitoring and reporting system:

1. Identification or alert of unusual activity which may include employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output.
2. Managing alerts or red flags.
3. SAR decision making.
4. SAR completion and filing.
5. Monitoring and SAR filing on continuing activity.

Additionally, an effective SAR program will consider the following items per FinCEN guidance:

- Development of company-specific 'red flags' or items that at face value appear suspicious and would trigger an investigation.
- Company specific training on SAR policies, procedures, and red flags to ensure all pertinent staff have adequate knowledge of both regulatory and company requirements.
- Ensure all reports used in monitoring contain sufficient contextual information about the customer (e.g., source of funds) or the counterparty beyond originator or beneficiary name (e.g., their address, the Bank Identifier Code of the originating/beneficiary bank).
- Ensure any company-specific red flags are adequately captured in reports and information reviewed.
- Ensure there are detailed procedures to escalate a transaction to the AML Compliance Officer for potential reporting. These escalation processes should include:
  - Review by senior management and legal staff (e.g., BSA compliance officer or SAR committee).
  - Criteria for when analysis of the overall customer relationship is necessary.
  - Criteria for whether and, if so, when to close the account.
  - Criteria for when to notify law enforcement, if appropriate.

- Ensure there are detailed procedures on investigative processes to examine all available facts to determine if a suspicious transaction is reasonable.
- Maintain a log of SARs considered but not filed. This item should summarize the above process of detection, escalation, investigation, and the ultimate determination of why the transaction was considered reasonable.
- Periodically review all available compliance resources to determine if they are sufficient to detect suspicious activity based on the company's total transaction volume, account size, and asset size. Resources must grow commensurate to transaction, asset, and account growth:
  - Resources include not only personnel used to manually detect and oversee the AML function, but also systems that can automatically detect and flag transactions for review.
  - Although it is appropriate to direct employees and trust officers at all levels of the organization to be alert and report any potentially suspicious activity, it is unrealistic to rely on this requirement as a primary mechanism to identify suspicious activity for companies with large account or transaction totals. A single employee conducting daily review of all prior day's transactions will likely not be considered sufficient.
- It is not sufficient to merely reject a transaction due to its suspicious nature, the company would then also have a duty to file a SAR.
- Appropriate procedures to maintain SAR confidentiality.
- Reporting mechanisms to the board or board-appointed committee.
- Establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects when appropriate, identifying unusual or potentially suspicious activity related to those subjects, and filing, as appropriate, SARs related to those subjects.
- Internal controls to ensure proper segregation of duties. For example, best practices indicate the person completing the SAR form should not be the same individual submitting the SAR:
  - A review process to ensure SARs are complete, thorough, timely, and include all known subject information. The importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible.
  - SARs should use Advisory Key Terms when applicable. A listing of all suspicious activity report advisory key terms and corresponding guidance can be found on FinCEN's website located at https://www.fincen.gov/resources/suspicious-activity-report-sar-advisory-key-terms.
- Banks/trust companies must retain copies of SARs and supporting documentation for five years from the date of filing the SAR.

<u>Foreign Financial Account Reporting</u>

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 U.S. 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.