TIMBERLAND BANK
Bank Secrecy Act/Anti Money Laundering Policy

In 1970, Congress passed the Currency and Foreign Transactions Reporting Act commonly known as the "Bank Secrecy Act" ("BSA"), establishing recordkeeping and reporting requirements by private individuals, banks, and other financial institutions. The BSA is intended to safeguard the US financial systems and the financial institutions that make up the system from the abuses of financial crimes, including money laundering, terrorist financing, and other illicit financial transactions.

It is the policy of Timberland Bank ("Bank") to comply with the letter and spirit of the BSA, USA PATRIOT Act, OFAC, and anti-money laundering laws. As a corporate entity, it is our responsibility to help deter crime. The Bank does not want to do business with suspected drug traffickers, money launderers, terrorists or other criminals, and will cooperate with law enforcement officials regarding suspected money-laundering schemes. This policy is designed to provide overall guidance to the Bank, its directors, management, and all employees in helping carry out our BSA/AML mission.

Requirements for the BSA/AML Compliance Program
The Federal Financial Institutions Examination Council ("FFIEC") and regulatory agencies have established five pillars, or expectations, that will help to ensure the Bank has an effective BSA/AML compliance programs. The Bank will ensure the BSA/AML Program meets each of these requirements:

Internal Policies, Procedures, and Controls
The Bank has established this BSA/AML Program to ensure the Bank is meeting the requirements for developing appropriate internal policies, procedures, and controls based on the Bank's structure, customer base, size, and BSA/AML and OFAC risk assessment.

Designation of a BSA/AML Compliance Officer
The Bank's BSA/Anti-Money Laundering ("AML") Officer, Melissa Eaton, is responsible for the quality of the overall state of BSA/AML compliance. The BSA/AML Officer coordinates and monitors daily BSA/AML compliance activities. The Board and senior management will ensure the BSA/AML Officer has sufficient tools and resources to administer an effective compliance program. If the BSA/AML Officer is not available, the BSA Manager will assume responsibility for the administration of the BSA/AML Program. If time sensitive issues arise the BSA Manager will report to Senior Management for guidance.

The Board of Directors will ensure the BSA/AML Officer has an appropriate level of authority and independence to comply with all of the BSA/AML requirements.

Ongoing Training
All bank personnel affected by the Bank Secrecy Act are required to receive annual training regarding the requirements of regulation. Within 30 days of hire and at least annually, each employee will successfully complete job-specific BSA/Anti-Money Laundering online training course through FIS Regulatory University. In addition, each employee will review this policy annually, acknowledging that they have read, understand, and will comply with the policy. The BSA/AML Officer will maintain these records for five (5) years.

Independent Audit

The Bank will ensure there is an annual independent testing for compliance with the Bank Secrecy Act, USA PATRIOT Act, OFAC and anti-money laundering laws. On-going monitoring will be performed by the BSA/AML Officer. The Bank's Audit Committee will review all audit reports.

Customer Due Diligence

To ensure compliance with the regulatory requirements for Customer Due Diligence, the Bank will understand the nature and purpose of each customer relationship. Ongoing monitoring of Bank relationships will be performed, to include updating appropriate customer information, as required, and reporting suspicious activity.

Additional information regarding the Bank's identification and verification procedures are located in the Board approved, Customer Identification Program ("CIP"), which includes the procedures for identifying beneficial owners on accounts for corporate entities and, in some cases, accounts held in the name of a trust. Beneficial owners are defined as persons who have 25% or more of the equity interests in the company AND/OR individuals with significant responsibility to control, manage, or direct the company – including executive officers, senior managers (for example, CEO, CFO, COO, Managing Member, General Partner, President, Vice-President or Treasurer). If a trust owns, directly or indirectly, 25% or more of the equity in a company, the trustees are considered beneficial owners.

The Bank also regularly monitors high-risk customers via Enhanced Due Diligence ("EDD") procedures. The goal of the Bank's EDD program is to ensure any customers who are determined to be of higher risk to the Bank are supplying sufficient documentation to support their activity and/or industry, and trigger accurate alerting and monitoring through the Bank's BSA/AML software.

Money Laundering

Money laundering is a process in which funds obtained from illegal activities are re-channeled to appear as if they were obtained through a legitimate business. Money laundering helps to disassociate a person from illegal income by hiding the paper trail connecting money to its original source. In the simplest money laundering scheme, funds from an illegal source are deposited in a bank and drawn out later in the form of a cashier's check. The Money Laundering Act of 1986 makes money laundering a federal crime, which includes engaging knowingly in a money laundering transaction involving property from criminal activity.

Structuring

Structuring is an attempt by a money launderer to avoid detection by engaging in cash transactions below the reporting threshold. For example, a customer who makes two $9,000 deposits at separate teller windows to avoid filing a Currency Transaction Report ("CTR") is structuring transactions. It is a federal crime to structure, attempt to structure, or to assist in structuring a large currency transaction to avoid filing a CTR. Bank personnel must never provide information that could assist a customer in structuring a transaction. For example, if a customer has $15,000 to deposit, do not advise the customer to deposit $9,000 today and $6,000 tomorrow.

"Smurfing"

A complicated money laundering scheme called "smurfing" involves couriers conducting numerous small currency transactions at banks in amounts below the $10,000 reporting threshold. In a typical operation, the couriers, or "smurfs", travel throughout the United States purchasing cashier's or traveler's checks, money orders, or negotiable Certificates of Deposit in amounts below the reporting threshold.

The Bank Secrecy Act requirements enacted in 1990 were specifically designed to deter and detect "smurfing" and other money laundering techniques. These requirements are commonly referred to as the "$3,000 rule." Money laundering usually involves one or more of the following activities:

- Placement - The process of placing, through deposits or other means, unlawful cash proceeds into traditional financial institutions.
- Layering - The process of separating the proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveler's checks, money orders, wire transfers, letters of credit, stocks, bonds, or purchasing valuable assets, such as art or jewelry.
- Integration - The process of using an apparently legitimate transaction to disguise the illicit proceeds, allowing the laundered funds to be disbursed back to the criminal. Different types of financial transactions, such as sham loans or false import/export invoices, can be used.

$3,000 Rule

The Bank Secrecy Act requires financial institutions to verify and retain records of the purchaser's identity when selling cashier's checks, traveler's checks, money orders, and bank checks and drafts in amounts of $3,000 to $10,000 in currency. See the Cash Sales of Monetary Instruments section for procedures concerning these transactions.

Funds Transfers

The Funds Transfer Recordkeeping rule requires financial institutions involved in a funds transfer to collect and retain certain information when the transactions are $3,000 and greater and for all international Automated Clearing House (ACH) transactions. See the Funds Transfers section for procedures concerning these transactions.

Providing Banking Services to Marijuana Related Businesses

The Controlled Substance Act ("CSA") makes it illegal under federal law to manufacture, distribute, or dispense marijuana. While federally illegal, many states have legalized certain marijuana-related activities. Washington State legalized the recreational use of marijuana in November 2012. In light of these developments, the US Department of Justice ("DOJ") Deputy Attorney James M. Cole provided updated guidance to federal prosecutors concerning marijuana enforcement under the CSA. FinCEN issued additional guidance on February 14, 2014 regarding the banking of marijuana related businesses. In January 2018, the DOJ rescinded all previously issued marijuana-related memos; however, FinCEN's guidance is considered to be valid and current guidance for the BSA/AML responsibilities relating to State-legal marijuana businesses. The Bank has established a Marijuana Banking Program to address some of the financial needs of the new and evolving marijuana-related industry in Washington State. The Bank will not initiate a lending relationship directly with a licensed marijuana business. Additional due diligence may be required on commercial loans that lease or rent space to marijuana related businesses; however, these indirect lending relationships are discouraged. Robust procedures and enhanced due diligence processes have been developed for restricted and limited marijuana related deposit accounts. See the Marijuana Related Business section for procedures related to services for these account types.

Customer Inquiries

If a customer asks any questions about the Bank's compliance with BSA, employees should simply respond that they are complying with federal law. Employees must never advise a customer on how to present currency in a manner to avoid the reporting threshold. **Doing so is a criminal act under federal law.**

Currency Monitoring System
The Bank will properly report all currency transactions that exceed $10,000 made by or for any person on any day, and retain required records of monetary instruments sold for currency in the amounts of $3,000 to $10,000. The Bank will identify and report multiple transactions made by or for any person on any day, which, when aggregated, exceed the reporting or recordkeeping limits. The Bank will also collect and retain Customer Identification Program information on all purchasers of monetary instruments and funds transfers of $3,000 and greater. Please refer to the Customer Identification Program procedures.

If the individual conducting the transaction is doing so on behalf of another person or entity, that third party's identity, Social Security or tax identification number, birth date, and account number must be obtained.

If the individual is a law enforcement or revenue officer performing a reportable transaction as part of their official duties, the Bank will verify that the person is an officer by inspecting a badge and other credentials.

When completing a CTR, the Bank Secrecy Act does not allow the Bank to accept a bank signature card as identification. Also, statements such as "known customer" or "bank signature card on file" are not permitted.

USA PATRIOT Act

Account Identification and Verification
The Bank will make every effort to comply with the USA PATRIOT Act through use of its customer identification and verification procedures and by consulting Control Lists for known or suspected terrorists or terrorist organizations. All new accounts will be carefully screened and reviewed to assess the level of risk that account may present to the Bank. All accounts identified as "higher" risk will be referred to the BSA/AML Officer for approval and account monitoring. Detailed information regarding the Bank's identification and verification procedures are located in the Customer Identification Program ("CIP") portion of the BSA/AML procedures**.**

Other Components of the USA PATRIOT Act
The Bank will make every effort to comply with all aspects of the USA PATRIOT Act, including sections 311, 312, 313, 314, and 319(b). Specific procedures to ensure compliance with the Act are contained in the Bank's Board approved BSA/AML compliance program.

Suspicious Activity Reports
The Bank will file a Suspicious Activity Report ("SAR") when it detects a known or suspected violation of federal criminal law as well as suspicious transactions related to money laundering offenses and violations of the Bank Secrecy Act. A SAR will also be filed when there is no business or apparent lawful purpose for the transaction(s) or the transaction(s) is not the sort in which the customer would normally be expected to engage (i.e., unusual behavior). The Board of Directors will be promptly notified when a SAR is filed. Procedures are in place for reporting unusual or suspicious activity; see the Suspicious Transactions section for additional details on the SAR Referral and SAR Committee process.

Office of Foreign Assets Control

The Bank will comply with the Office of Foreign Assets Control ("OFAC") rules, which administers a series of laws that impose economic sanctions against target hostile foreign countries to further U.S. foreign policy and national security objectives. The BSA/AML Officer is designated as the Bank's OFAC Officer and is responsible for monitoring and coordinating day-to-day compliance with the OFAC laws and regulations.

The Bank may be subject to additional enforcement actions for failure to comply with OFAC requirements. These enforcement actions can include civil monetary penalties as great as $250,000 per violation or twice the amount of a transaction, whichever is greater. Maintaining an adequate OFAC compliance program and adhering to the OFAC procedures will help to protect the Bank from these types of actions.

Risk Assessment and Analysis

The Bank has developed a BSA/AML and OFAC Risk Assessment and Analysis to assist the Bank and employees in mitigating the risks posed by potential customers and to ensure existing accounts and transactions are monitored to identify any suspicious activity. When completing the assessment, management considered the risks both individually within the business or product line and across the company as a whole. This risk assessment will be reviewed, at a minimum, annually and will be approved by the Board of Directors. It will also be reviewed whenever the Bank offers a new product or business line to ensure any new risks or mitigating factors are considered. It will be updated, as required, based on audit or regulatory agency examination findings.

Penalties for Non-Compliance

The Bank and its officers, directors, and employees are subject to significant civil and criminal penalties for violation of the Act or its regulations. Civil penalties can be as large as $215,628 for willful violations of the law. Bank employees may be liable for being "willfully blind" if they suspect a customer is attempting to circumvent the recordkeeping or reporting requirements of the BSA but fail to investigate or report these suspicions to law enforcement officials. Criminal penalties include fines from $1,000 to $500,000 and jail terms of up to ten years for violating the criminal provisions of the BSA. Failure to complete a CTR when required will result in an oral warning to the employee. After a second failure, the employee will be given a counseling letter. A third failure will have the employee placed on probation. A fourth failure may lead to dismissal. Any employee who intentionally fails to comply with the Bank's policies and procedures regarding the Bank Secrecy Act is subject to immediate dismissal**.**

Customer Identification Program

General

When opening a new account for a legal entity, the Bank will obtain a statement from an authorized person as to all individuals who have beneficial ownership of 25% or more in the company. The authorized person will sign a statement certifying this information is true to the best of their knowledge. This statement will be retained by the Bank as part of the new account opening documents, subject to the recordkeeping requirements of the regulations.

When the BSA was first enacted in 1970, its primary purpose was to help deter white-collar crime such as income tax evasion by furnishing law enforcement agencies with more evidence of financial transactions. In addition, the BSA provided the government with information about the use of secret foreign bank accounts.

Since its enactment, the BSA's recordkeeping and reporting requirements have evolved into a law enforcement tool used to curb drug-related money laundering. Over the years, this use of the BSA has brought banks into the middle of the nation's "war on drugs." However, the events of September 11, 2001 triggered a need to strengthen and broaden the BSA's utility and effectiveness.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism ("USA PATRIOT Act") was signed into law on October 26, 2001. The Act was designed to deter and punish terrorist acts in the U.S. and around the world and to enhance law enforcement investigatory tools. Section 326 of the USA PATRIOT Act sets forth standards for financial institutions to follow in the identification and verification of customers at account opening. Compliance with the USA PATRIOT Act was required by October 1, 2003.

The USA PATRIOT Act requires the Bank to implement a written Customer Identification Program ("CIP") appropriate to its size, location and type of business. Furthermore, the Act mandates that the Bank will establish account opening procedures, which include collecting certain information before opening an account, verifying the collected information within a reasonable time, and having a CIP that addresses all aspects of the Bank's customer due diligence program. The CIP must also be approved by the Board of Directors as part of the Bank's overall Anti-Money Laundering ("AML") and BSA program.

Effective May 11, 2018, the Bank is required to identify beneficial owners of all accounts (deposit, loan, private banking, trust, cash management, etc.) for legal entities. This means the Bank must obtain information from the legal entity that identifies the natural persons who own 25% or more of legal entity. Identification of the beneficial owners is obtained from an authorized representative of the entity. A Certification Form is completed and signed by that person. The accuracy of that statement can be relied upon, unless the Bank has reason to believe the statement is not accurate. Once the beneficial owners have been identified, verification of their identity must be conducted. These identification and verification steps must be completed each time a new account is opened, even the legal entity is already a customer of the Bank. The Bank cannot rely on information previously provided. Verification of the beneficial owners can be performed using documentary or non-documentary methods.

Policy Elements and Goals

Timberland Bank ("Bank") is committed to the concept of identifying and verifying customers who use the Bank's many services and products. The CIP procedures will ensure the Bank verifies the identity of each customer to the extent reasonable and practicable.

The intent of the Bank's CIP policy is to minimize the risk of fraud, discourage criminals from using the Bank for other illicit purposes (such as money laundering), and assist in the fight against terrorism.

Elements

The following elements make up the Bank's CIP policy.

- The Bank will verify the identity of any person seeking to open an account, including the beneficial owners of an account for a legal entity, to the extent reasonable and practicable.
- When opening a new account for a legal entity, the Bank will obtain a statement from an authorized person as to all individuals who have beneficial ownership of 25% or more in the company. The authorized person will sign a statement certifying this information is true to the best of their knowledge. This statement will be retained by the Bank as part of the new account opening documents, subject to the recordkeeping requirements of the regulations.
- The Bank will maintain records of the information used to verify a person's identity, including name, address, and other identifying information.
- The Bank will determine whether the person appears on any list(s) required under Section 326 of known or suspected terrorists or terrorist organizations provided to the Bank by any government agency.
- The Bank will determine the level of risk presented by each account. Additional verification measures will be taken for all business accounts and for all accounts that are identified as a higher risk or potentially higher risk account.

Goals

By following each element of the CIP policy, the Bank will achieve the following goals.

- Assure the Bank is in compliance with the BSA, USA PATRIOT Act, and other anti-money laundering laws and regulations, which helps to reduce the Bank's exposure to monetary penalties for noncompliance.
- Decrease the likelihood of the Bank becoming a victim of fraud, terrorist activity, money laundering or other illegal acts or schemes.
- Reduce the risk of Bank losses from government seizure and forfeiture of a customer's loan collateral when the customer is involved in illegal activity.
- Prevent the Bank's public image from becoming associated with criminal activity.
- Assure the Bank can readily identify suspicious and/or unusual activity (activity different from a customer's regular banking transactions).

Definitions

Account

An account is a formal ongoing banking relationship established to provide or engage in services, dealings, or other financial transactions including:

- Deposit, transaction or asset, credit accounts, or other extensions of credit.
- Safe deposit box or other safekeeping services.
- Cash management, custodian, and trust services.
- Prepaid access cards, when the Bank has an ongoing relationship with the holder/purchaser.

An account does not include:

- Products/services where a formal banking relationship is not established (e.g. check cashing, wire transfers, sale of checks or money orders).
- Accounts acquired through acquisitions, mergers, purchases of assets, or assumption of liabilities from a third party.
- Accounts opened for the purpose of participating in employee benefit plans established under the Employee Retirement Income Security Act of 1974 (ERISA).

Customer

The term "customer" includes:

- A person that opens a new account. A "person" includes individuals, corporations, partnerships, trusts, estates, joint stock companies, associations, syndicates, joint ventures, other unincorporated organizations or groups, certain Indian Tribes, and all entities recognized as legal persons.
    - For personal accounts, each person named on a joint account is considered a "customer".
    - For commercial accounts, the business entity is considered the "customer" (not the individual signatories); however, all beneficial owners and authorized signers will be fully identified.
- An individual who opens a new account for a person lacking legal capacity or an entity that is not a legal person (e.g. a minor or an entity that is not a legal person, such as a civic club or bowling league).

The term customer does not include:

- Financial institutions regulated by a Federal functional regulator or a state regulator.
- Governmental agencies and listed companies (New York Stock Exchange, American Stock Exchange, NASDAQ National Market Security listed on the NASDAQ Stock Market) to the extent of their domestic operations.
- Persons with an existing account, provided the Bank has a reasonable belief that it knows the customer's true identity.
- A person who does not receive banking services, such as a person whose loan application was denied.

Beneficial Owners of Legal Entities

Beneficial owners are defined as persons who have 25% or more of the equity interest in the legal entity AND/OR individuals with significant responsibility to control, manage, or direct the legal entity – including executive officers, senior managers (for example, CEO, CFO, COO, Managing Member, General Partner, President, Vice-President or Treasurer). If a qualifying trust owns, directly or indirectly, 25% or more of the equity in a company, the trust is considered a beneficial owner and the trustee(s) must be identified.

The following type of customers are not included in the regulatory requirements for identification of beneficial owners:

- Sole Proprietorships
- Unincorporated Associations – such as Scout Troops, youth sports groups, and small local community associations.

- Trusts – other than statutory trusts created by the filing with a Secretary of State or similar office.
- A financial institution regulated by a Federal functional regulator or a bank regulated by a State bank regulator.
- A department or agency of the United States, or any State, or any political subdivision of any State (county, city, township, etc.)
- Any entity established under the laws of the United States, of any State, or of any political subdivision of any State, that exercises governmental authority on behalf of the United States, or any such political subdivision.
- Any entity, other than a bank, whose common stock or analogous equity interests are listed on the New York Stock Exchange, or the American Stock Exchange, or whose common stock or analogous equity interests have been designated as a NASDAQ National Market Security listed on the NASDAQ Stock Market (except stocks listed under the separate "NASDAQ Capital Markets Companies" headings).
- Any subsidiary, other than a bank, or any entity described above, that is organized under the laws of the United States, or of any State, and at least 51 percent of whose common stock or analogous equity interest is owned by the listed entity.
- An issuer of a class of securities registered under Section 12 of the Securities and Exchange Act of 1934.
- An investment company as defined in Section 3 of the Investment Company Act of 1940 that is registered with the Securities and Exchange Commission.
- An investment advisor, as defined in Section 202(a)(11) of the Investment Advisors Act of 1940 and is registered with the Securities and Exchange Commission.
- An exchange or clearing agency as defined in Section 3 of the Securities Exchange Act of 1934.
- A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant each as defined in Section 1a of the Commodity Exchange Act that is registered with the Commodity Futures Trading Commission.
- A public account firm registered under Section 102 of the Sarbanes-Oxley Act.
- A bank holding company, as defined in Section 2 of the Bank Holding Company Act of 1956, or savings and loan holding company as defined in Section 10(n) of the Home Owner's Loan Act.
- A pooled investment vehicle that is operated or advised by a financial institution regulated by Federal functional regulator or by a State bank regulator.
- An insurance company that is regulated by a State.
- A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010.
- A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution.
- A non-US governmental department, agency, or political subdivision that engages only in governmental rather than commercial activities.
- Any legal entity only to the extent that it opens a private banking account subject to the due diligence requirements for private banking accounts within the BSA.

Customer Due Diligence and Identification Procedures

The initial Customer Due Diligence (CDD) process will assist the Bank is identifying, detecting, and evaluating unusual or suspicious activity. Any customers who are identified as higher risk or potentially higher risk are subject to Enhanced Due Diligence efforts.

The Bank will verify the identity of each customer to the extent that is reasonable and practicable prior to account opening. The verification process will be risk-based and enable the Bank to form a reasonable belief that it knows the true identity of each customer. The Bank will consider the following in determining the risk associated with the account:

- Whether the account being opened is for a new or existing customer – New customers pose a higher risk to the Bank.
- The type of account that is being opened.
- The methods of account opening – Applications received by mail, telephone or the Internet are higher risked.
- The location of the customer or business – Non-local customers (i.e. out of state, foreign) are a higher risk to the Bank.
- The citizenship or country of organization – Non-U.S. citizens or businesses are a higher risk to the Bank.
- The type of business or expected transactions.
- Established customers that are changing their address.
- If the commercial customer provides Internet gambling services. See the Bank's Regulation GG Policy and Procedures for further details.

Cash intensive businesses are higher-risk accounts. These businesses easily allow for the conversion of cash into other assets or are vulnerable to being used to facilitate money-laundering activity. Examples of cash intensive businesses include: Money Service Businesses (MSBs); Casinos; Dealers in precious metals, stones, or jewelry; Sellers of vehicles, including autos, airplanes, and boats; Pawn brokers; Travel agencies; Currency exchanges; Gas stations or mini marts; Restaurants; Charitable organizations; Offshore corporations; Art/antique dealers; marijuana-related businesses, and Import/Export businesses.

All higher-risk accounts are subject to enhanced due diligence at the time the account is opened. All higher-risk accounts will be identified and reported to the BSA/AML Officer. Higher-risk accounts are monitored on a regular basis to detect suspicious account activity.

Please note: If you are opening a new account and you do not feel comfortable with the person(s), documentation, and/or business, contact the BSA/AML Officer or the BSA Manager prior to opening the account.

The mandatory account opening procedures relate only to new accounts. However, if the Bank does not have a reasonable belief that it knows the true identity of an existing customer, the Bank will verify identification for new accounts opened by existing customers.

The Bank has developed customer profile questionnaires that will be completed for each new business customer, with additional information requirements for each new business customer who operates a money services business. Additional due diligence collected is maintained in the Bank's BSA software.

Nonbank Financial Institutions

A Nonbank Financial Institution ("NBFI") is broadly defined as a business other than a bank that offers financial services. Common examples of NBFI's include, but are not limited to:

- Money services businesses ("MSB") See below for additional information for MSB accounts.
- Casinos and card clubs
- Securities and commodities firms (broker/dealers, investment advisors, mutual funds, hedge

funds, or commodity traders)
- Insurance companies
- Other financial institutions (e.g. dealers in precious metals, stones or jewels, pawn brokers, loan or finance companies)

Some NBFI's are required to develop an AML program and comply with the reporting and recordkeeping requirements of the Bank Secrecy Act and anti-money laundering laws. However, they typically need to have access to traditional financial institutions in order to conduct business. While the BSA, regulatory agencies and FinCEN do not expect banks to serve as an additional regulatory agency, they are expected to identify and manage the risks these types of customers present.

The size and complexity of the services offered by NBFI will determine the level of risk these customers may present. A large multi-national corporation presents a higher level of risk than a small, independent business that cashes checks for their customers. The range of products and services offered and the customer base of the NBFI are the first factors to consider when determining any risks maintaining an account relationship will present to the Bank. Some of these risk factors these types of business present that may increase the risk of the account being used for money laundering purposes are:

- They engage in transactions without establishing on-going relationships and requiring minimal or no identification when their customer completes a transaction, including currency transactions.
- They may maintain limited or inconsistent records for transactions and customer histories
- They are subject to varying levels of regulatory requirements, oversight, and examination
- They can quickly and easily change their products or services.
- They can quickly close their businesses with little or no notice.
- They may operate without obtaining the proper registration or licensing.

To mitigate the risks posed by maintaining an account for a NBFI, the Bank will:

- Identify all NBFI relationships.
- Assess the potential risks posed by each relationship.
- Conduct initial and ongoing due diligence for these relationships.

The following factors will be considered when opening a new account for a NBFI:

- The types of products and services they offer.
- The number of locations and markets served by the NBFI.
- The anticipated account activity.
- The purpose of the account(s).

Money Services Businesses

In 2005, FinCEN and the federal banking agencies published guidance to clarify the BSA/AML requirements and supervisory expectations for accounts opened or maintained by a MSB. Many MSBs are subject to the full range of BSA requirements, including currency transaction reporting, detecting and reporting suspicious activity, developing an effective AML program, and some identification and recordkeeping rules. All MSBs must register with FinCEN, unless they are operating as an agent for another MSB. Many states also require the MSB to be licensed in the state(s) in which they are incorporated or where they are operating.

The following are the regulatory expectations for Banks who maintain accounts for a MSB:

- The Bank will manage the risks associated with all MSB accounts, but it is not responsible

for the MSB's BSA/AML Program. However, if the risk assessment for a MSB customer indicates they pose a higher level of risk to the Bank, reviewing their BSA/AML Program should be included in the enhanced due diligence process.

- Not all MSBs pose the same level of risk or require the same level of due diligence. If the Bank's risk assessment for a MSB customer indicates they are lower risk for money laundering or other illegal activities, enhanced due diligence measures are not required.

MSB Risk Assessment

The Bank must assess the risk each MSB customer presents when agreeing to service accounts for the MSB. The purpose of the account, the anticipated account activity, the types of products and services the MSB offers, and the locations and customer base the MSB serves are good starting points for determining the level of risk. Each element should be considered. If the risk assessment indicates the account may present a higher level of risk to the Bank, enhanced due diligence should be performed before opening the account(s). Some of the factors that may reduce or mitigate the risks an MSB presents include:

- The MSB is currently registered with FinCEN.
- The MSB has obtained any required state or local business licenses and registrations.
- The MSB has already developed an AML program.
- The MSB has been examined by the state or IRS with positive examination results.
- The MSB currently has established banking relationships that are in good standing.
- The MSB is an established business with an operating history.
- The MSB provides services only to local residents.
- Most of the MSB's customers conduct routine transactions in low dollar amounts.
- The MSB's account history is consistent with the expected level of activity that was determined when the account was opened.
- The MSB performs lower-risk services, such as cashing government or payroll checks and check cashing services are not offered for third-party or out of state checks.
- If the MSB provides money transmitting services, they are primarily to domestic locations and/or are limited to lower dollar amounts.
- The MSB operates solely as an agent for another large, widely recognized MSB, such as Western Union.

Due Diligence for MSB customers

At a minimum, the Bank will require the following from all potential MSB customers:

- Compliance with the Bank's CIP requirements for a business account.
- Confirmation that the MSB is registered with FinCEN. MSB's operating as an agent for another MSB are not required to register with FinCEN. If the potential MSB customer is an agent for another MSB, the Bank will obtain confirmation of current agent status.
- Obtain copies of any applicable state or local licenses and registrations required to operate the MSB or MSB portion of their business.
- Complete a basic risk assessment to determine the level of risk the new account may present to the Bank and determine if further due diligence is required.

The Bank will file a SAR if it becomes aware of a MSB customer that is operating a business in violation of the FinCEN registration or state licensing requirements.

The mandatory account opening procedures relate only to new accounts. **However, if the Bank does not have a reasonable belief that it knows the true identity of an existing consumer customer, the Bank will verify identification for new accounts opened by existing consumer customers. All accounts for legal entities will be subject to the new account opening procedures each time a new account is established.**

Enhanced Due Diligence

Higher risk accounts and potentially higher risk accounts are subject to Enhanced Due Diligence ("EDD"). The purpose of performing EDD is to ensure the Bank has sufficient information to be able to determine the identity of the account holder and that the Bank has a basis for evaluating "normal" account activity for higher risk accounts. Annual on-site visits to Money Service Business account holders may occur. On-site visits may be performed, as needed, for other accounts identified as higher risk or potentially higher risk.

Higher risk or potentially higher risk accounts are accounts that are opened for cash intensive businesses, private banking accounts, private investment companies ("PIC"), professional service providers, marijuana-related businesses, foreign correspondent accounts, and accounts for non-US persons or businesses, including politically exposed persons. They also include accounts opened with exceptions to the Bank's CIP (requires approval from the BSA/AML Officer), accounts that have been identified as higher risk through the review of the customer profile, through account transaction monitoring, and accounts held by subjects of a Suspicious Activity Report filed by the Bank.

Some of the information that will assist the Bank in performing EDD on higher risk accounts includes:

- the customer's financial resources;
- the customer's occupation or the type of business;
- the purpose of the account;
- the expected transaction activity (amount, frequency, location);
- other banking relationships; approximate salary or annual sales; and
- the beneficial owners of the account (if applicable).

Enhanced Due Diligence for a MSB Account

If a potential MSB customer presents a potentially higher level of risk to the Bank, for example it does not meet the risk mitigating factors listed above, additional due diligence is required. The size of the MSB and the types of products it offers may also impact the level of risk. Different types of MSB activity present different risks. A local grocery store that will cash payroll checks for customers who are buying groceries presents a significantly lower level of risk than an MSB customer who transmits cross-border funds transfers. If the risk assessment indicates further due diligence is necessary, the Bank will complete the following, as applicable:

- Review the MSB's AML Program to ensure it meets the guidelines established by FinCEN.
- Review the results of the last independent testing of the MSB's AML program.
- Conduct an on-site visit.
- Ensure the MSB has written operating procedures and review these procedures to ensure they provide adequate BSA/AML guidance.
- Review written employee screening practices for the MSB.
- If the MSB provides services through agents, review the list of agents operating within or outside of the United States, which will be receiving services directly or indirectly through

the MSB account. Written agent management and termination practices will also be reviewed.

Enhanced Due Diligence for Marijuana-Related Businesses

Due to the federally high risk nature of a marijuana-related business, additional and ongoing due diligence is required. The size of the marijuana-related business may also impact the level of risk. Licensed marijuana business accounts are required to have SARs filed every ninety (90) days with specific language addressing the federal enforcement priorities addressed in FinCEN guidance. At a minimum, the Bank will require the following from marijuana-related businesses:

- Compliance with the Bank's CIP requirements for a business account
- Additional enhanced CIP safeguards detailed above for each account type
- Detailed quarterly account review
- Marijuana Related Business Questionnaire
- Annually, all licensed entities will be required to sign a new WSLCB release form requesting any file changes from the initial application to confirm that Bank CIP records are consistent with State records.

Required Customer Information to be Collected

The Bank will obtain, at a minimum, the following required information from the customer prior to opening an account. This information will also be obtained for beneficial owners and authorized signers. If the owner/signer is not present, and with management approval, an account for a legal entity can be opened prior to obtaining this information from every owner/authorized signer.

- Name
- Date of birth – (Not required for business accounts)
- Address
    - For an individual, an actual residential or business street address.
    - For an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, the residential or business street address of next of kin or of another contact individual, or a description of the customer's physical location.
    - For a person other than an individual (such as a corporation, partnership, or trust), a principal place of business, local office, or other physical location.
- Identification number
    - For a U.S. person (those persons that are U.S. citizens and businesses, and other entities that are organized under the laws of a State or of the U.S.):
        - A social security or taxpayer identification number ("TIN").
    - For a non-U.S. person, one of more of the following:
        - A taxpayer identification number.
        - Passport number and country of issuance.
        - Alien identification card number.
        - Number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. Note: When opening an account for a foreign business or enterprise that does not have identification number, the Bank will request alternative government-issued documentation certifying the existence of the business or enterprise (i.e. business license).
    - The Bank may open an account for a customer (individual or business) that has

applied for, but has not received, a social security or taxpayer identification number. However, the Bank will confirm that the application was filed before the customer opens the account and obtain the social security or taxpayer identification number within **30 days** after the account is opened. If the identification is not received within the required time frames, the account will be closed.

- If this information is not available for every beneficial owner and authorized signer on a business account at the time the account is opened, the Bank will require the information be provided within **30 days** after the account is opened. If this information is not provided for a beneficial owner, the account must be closed if the information is not received within this time frame. If the information is not provided for an authorized signer, the Bank will notify the business that individual will not be allowed to access the account.
- A statement from all new commercial customers stating whether they do or do not offer Internet gambling services when the Bank determines the business is not a minimal risk. Please see the Regulation GG Unlawful Internet Gambling Enforcement Act policy for more details.

Based on its assessment of risk, the Bank may require identifying information in addition to the items above for certain customers or product lines.

Verification Procedures

In addition to collecting the required information discussed above, the Bank will verify the identity of the customer using that collected information. The required verification will occur within a reasonable time after the account is opened.

Verification through Documents

One or more of the following documents will be used to verify a customer's identity. The Bank may use other documents, provided they allow the Bank to establish that it has a reasonable belief that it knows the true identity of the customer. Given the availability of counterfeit or fraudulently obtained documents, the bank is encouraged to obtain more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity.

- For individuals:
  - An unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license, passport or military ID.
- For a person other than an individual (such as a corporation, sole proprietorship, partnership, or trust):
  - Documents showing the existence of the entity, such as articles of incorporation, corporate or partnership resolutions, an unexpired government-issued business license, a partnership agreement, or a trust instrument.

When a customer presents identification, the document should be thoroughly examined. The photograph and description on the identification must be consistent with the appearance of the person who presents it. The following steps should be taken when examining a customer's identification:

- Compare the photograph with the customer to confirm the photograph is that of the customer.

- Compare the physical data to the customer's appearance. Physical data includes features such as height, weight, and eye color.
- Check the ID issue date. Newly issued ID could signal potential problems.
- Check the ID expiration date.
- Check the overall appearance of the ID. Run your finger around the edge of any laminate to detect breaks. Examine official seals, holograms, and special features to ensure they look genuine.

If the identification presented appears to be altered or counterfeit, contact the **BSA Manager, Deposit Operations Administrative Team or BSA Officer** for assistance.

Verification through Non-Documentary Methods

For accounts opened by telephone, mail or over the Internet, the Bank will use one or more of the following methods to verify the identity of its customers. These methods will also be used if the Bank is unfamiliar with or questions the validity of any documents received or is presented with circumstances that increase the risk that it will not be able to verify the true identity of the customer through documents (e.g. attorney in fact accounts). These methods will be used in addition to, or instead of, relying on documents.

- Contacting the customer after the account is opened (e.g. thanking the customer for opening the account and asking if there is any other service the Bank could provide).
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency (positive verification), public database (negative verification), or other source.
- Verifying a home address using a reverse directory, city directory, telephone book, or mail drop list (logical verification).
- Verifying a customer's employment by contacting the current employer.
- Verifying home and work telephone numbers by calling the number and asking for the customer.
- Obtaining a financial statement.
- Checking references with other financial institutions.
- Establishing the purpose of a loan, regardless of the collateral.

For business accounts, the Bank will also consider utilizing one or more of the following methods to identify beneficial owners and/or authorized signers on the account:

- Independently verifying the beneficial owner/authorized signer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency (positive verification), public database (negative verification), or other source.
- Conduct a site visit of the place of business.
- Visit the business website or send a confirming electronic message to the business e-mail address.

In some instances, exceptions may be made for customers that do not have an unexpired government-issued identification (e.g. an elderly or disabled person, Amish or other special interest groups). The account may be opened if the Bank is confident that they have reasonable belief that they know the true identity of the customer. The employee will review the Bank's internal records for any information on

file and ask for other forms of identification (e.g. expired government identification with photograph, school identification with photograph, etc.).
Another document must also be reviewed that contains both the customer's name and address. Examples of secondary identification include:

- Organizational membership card.
- Senior citizen identification.
- Medicare/Medicaid card.
- Voter registration card with signature and consistent information
- Utility bill.
- Real estate tax bill.
- Known employer ID card.
- Union card with signature.
- Credit card with signature.
- Gun permit with consistent information.

Additional Verification for Non-individuals

Based on the Bank's risk assessment of a new account that is opened by a corporation, business, trust or other similar entity, the Bank will obtain additional information about the business and, in some cases, the individuals with authority or control over the account, in order to verify the business's identity. For example, additional due diligence would be appropriate if an account is opened in the name of a corporation, partnership, or trust and is created or conducts substantial business in a jurisdiction that has been designated by the U.S. as a primary money laundering concern or has been designated as non-cooperative by an international body. The Bank needs to obtain information about, and verify, the identity of a sole proprietor or the principals in a partnership when the Bank cannot otherwise satisfactorily identify the sole proprietorship or partnership.

Depending on the type of account or other factors, it may be desirable for the Bank to also obtain information regarding:

- Whether the business is a holding company for assets owned by affiliated organizations.
- The primary type of activity the business engages in and whether its operations are primarily domestic or international.

Additional Safeguards for Marijuana Related Businesses

The Bank restricts the marijuana related deposit accounts to entities located in Washington State and relies on information from the Washington State Liquor and Cannabis Board ("WSLCB") for a portion of the CIP requirements. Complete details of the requirements for each type of account are documented in the Bank's Marijuana Related Banking Program. In addition to the standard verification procedures for non-individuals, due to the current conflict between State and Federal law and the high risk nature of the business type, marijuana-related business customers must provide the following additional information:

Licensed Entities

- Green Business Account Application
- Washington State Business License with a WSLCB Marijuana Addendum
    - Verification through inquiry on the WSLCB page (http://lcb.wa.gov/records/frequently-requested-lists) that shows the pending and/or approved application in process is acceptable. Accounts opened with a pending status will be verified every 90 days for

approval. If the application is ultimately withdrawn or denied, the account must be closed immediately.

- WSLCB Application packet, obtained directly from the WSLCB. The WSLCB performs security-related verifications that assist in CIP, such as criminal history/background checks, credit checks, and site location verifications.

Non-Licensed Entities

- These companies are not selling cannabis or marijuana plant product but may provide services or related products. Normal business CIP safeguards, including anticipated account activity, are considered adequate for these businesses.

Timberland will not initiate a lending relationship directly with a licensed marijuana business. Additional due diligence may be required on commercial loans that lease or rent space to marijuana businesses; however these indirect lending relationships are discouraged. The limit of total marijuana related deposit account balances is restricted to $65 million.

Additional Safeguards for Loan Customers

Loan safeguards, in addition to those previously mentioned, can help protect the Bank from losing collateral in a government forfeiture. Although these safeguards are not required under the CIP, the loan officer may want to consider taking additional steps based on risk (i.e. concerns have been identified during the loan application process, etc.) Such general safeguards include:

- Obtaining a written statement from the borrower regarding the legality of business activities, the intended legal use of the loan proceeds, and the fact that there are no pending or threatened legal proceedings that could result in forfeiture.
- Including covenant and default provisions in loan documentation that stipulate a borrower will not violate any law that could result in forfeiture and will provide the Bank with notice of any pending or threatened legal action.

Steps for Business Loans

For business loans, additional steps could include establishing an in-depth review of the customer's business, as well as investigating the customer's reputation in the business community or industry.

Collateral for Cash Loans

The Bank will exercise caution when granting "cash loans" if they are fully covered by collateral such as deposit accounts, securities, or other cash equivalents that are normally viewed as risk free. Collateral that is later traced to illegal activity may be subject to government seizure and forfeiture. As a result, the Bank would effectively have an unsecured loan.

Lack of Verification

If the Bank does not have a reasonable belief that they know the true identity of the customer (including beneficial owners and authorized signers) after completing the customer identification and verification process, the account will not be opened. The Bank will refuse to conduct business with any business that refuses to provide sufficient background information or credentials, or with any individual who refuses to provide proper identification.

There may be instances when an account will be opened while the Bank is in the process of identifying the customer. This will be considered an exception to the Bank's CIP policy and will be risk-based. Management will approve these exceptions and appropriate follow-up will be performed to ensure all information is obtained within a reasonable period of time, generally 30 days or less. Management will also determine if limits will be placed on the account until the customer's identity is verified (i.e. restricting the number and/or dollar amount of transactions). If the information cannot be obtained, the account will be closed.

The BSA/AML Officer will be notified immediately if an employee becomes aware of any unusual and/or suspicious activity. The BSA/AML Officer will investigate the circumstances and determine whether the account will be closed and/or if a Suspicious Activity Report ("SAR") will be filed. See the Bank's BSA/AML procedures for further information regarding suspicious activity.

Record Retention

The Bank will maintain records of all documents used in verifying the identity of the customer. The following records will be maintained:

- All identifying information about a customer. This information will be maintained for five years after the account is closed.
    - Name.
    - Address.
    - Date of birth.
    - Identification number.
- All information that verifies a customer's identity. This information will be maintained for five years after the account is closed.
    - A description of any document relied on to verify identification, including:
        - The type of document.
        - An identification number contained in the document.
        - The place and date of issuance (if any).
        - The expiration date.
    - A description of the methods and results undertaken to verify the identity of the customer when the Bank utilizes non-documentary or additional methods for verification (e.g. credit reports, references, etc.)
    - A description of the resolution of any substantive discrepancy discovered when verifying the information provided by the customer. For example, a notation that the Bank closed an account that it had opened when they could not verify the address and identification number provided by a customer that opened an account via mail.

Government Lists

The BSA Department will be responsible for determining whether a Bank customer appears on the Office of Foreign Asset Control list required under Section 326 of known or suspected terrorists or terrorist organization issued by any Federal government agency and designated as such by the Department of the Treasury in consultation with the Federal functional regulators.

The BSA Department will make the determination within a reasonable period of time after the account is opened, or earlier, if required by another Federal law or regulation or Federal directive issued in connection with the applicable list. The BSA/AML Officer will follow all federal directives issued in connection with any government list.

Customer Notice

Prior to opening an account, each customer will be provided notice that the Bank is requesting information to verify his or her identity. Depending on the manner in which the account is opened, the Bank will satisfy the notification requirement by posting a notice in the lobby or on its website; including the notice on its account applications; reading the notice for telephone applications; or using any other form of written or oral notice. Timberland Bank's practice is to provide a copy of the written notice to all account owners who are not present at the time the account is opened.

The notice will state:

> IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT
>
> To help the government fight the funding of terrorism and money laundering activities, Federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account.
> What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

Timberland Bank will not rely on another financial institution (including affiliates) to perform its CIP procedures.

The Bank is permitted to arrange for a car dealer or mortgage broker, acting as its agent in connection with a loan, to verify the identity of its customer. However, as with any other responsibility performed by an agent, the Bank is ultimately responsible for that agent's compliance with the requirements of this final rule. The Bank will establish adequate controls and review procedures for such relationships. Currently, the Bank is not involved in this activity.

Suspicious Transactions

General

Bank employees, across all business lines, need to be alert to detect transactions that are suspicious. A suspicious transaction may be an attempt to avoid the filing of a CTR, purchasing multiple monetary instruments for amounts under $3,000 over a short period of time, presenting a check that appears to be counterfeit, providing false information when applying for a loan, receiving or sending wire transfers or ACH transactions that are not consistent with the customer's usual activity, or any other activity that presents a high level of risk to the Bank.

When confronted with a suspicious transaction, the transaction should be processed in a normal manner and reported to the BSA/AML Officer. Surveillance systems are in use at all Bank locations and can capture the image of customers conducting transactions; recorded camera footage can be obtained when necessary. The BSA/AML Officer will investigate the transaction and determine if the transaction requires further action, to include reports to law enforcement. The BSA/AML Officer will report any confirmed suspicious activity to Financial Crimes Enforcement Network ("FinCEN") by completion of a Suspicious Activity Report ("SAR"). SARs will be filed when there is a reasonable basis to believe that the Bank was an actual or potential victim of the criminal violation or was used to facilitate the criminal violation. If the Bank believes the activity is suspicious and a logical reason for the activity cannot be discovered, a SAR will be filed. A SAR will be filed when there is no business or apparent lawful purpose for the transaction(s) and the transaction(s) is not the sort the customer would normally be expected to complete (i.e., unusual behavior).

As a prudent banking practice, employees will immediately report any transaction that seems suspicious, or questionable, even if the amount involved is less than $5,000. A transaction is suspicious if it has one or more of the characteristics listed in Appendix A.

The Bank will also use automated systems and BSA/AML software to aid in the detection, tracking, and reporting of suspicious activity. All inquiries from law enforcement regarding suspected criminal activity will be reviewed to determine if a SAR should be filed. Law enforcement inquiries include, but are not limited to, subpoenas, seizure warrants, and 314(a) list inquiries. The BSA/AML Officer, or her designee, is responsible for reviewing the automated systems and reports. The BSA/AML Officer will be notified when the Bank receives a subpoena or seizure warrant from law enforcement.

The BSA/AML Officer has established procedures and processes that ensure all referrals of potentially suspicious activity (from employees or electronic monitoring) are reviewed and evaluated on a timely basis. Personnel reporting suspicious activity will use the SAR Referral Form or electronic reporting through the Bank's BSA software to document the activity they have observed as unusual or suspicious. The SAR Referral will be reviewed by the BSA Officer, or her designee, and forwarded to the SAR Committee for determination of filing status. The SAR Committee is comprised of the BSA Officer, the BSA Manager, and the Chief Operating Officer; the BSA Officer may agree or disagree with the SAR Committee decision and may continue with filing appropriate reports as she deems necessary. Any deviation from the SAR Committee decision will be documented with the Bank's BSA Software. Documentation is retained to evidence these reviews.

Filing a SAR

A SAR must be filed and sent to FinCEN in the following circumstances:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more where a suspect can be identified.

- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act or its implementing regulations.
- Licensed Marijuana Businesses Alerts, including one of three statuses: 1) Marijuana Limited, 2) Marijuana Priority, or 3) Marijuana Termination
    - Note: SARs must be filed every 90 days on all licensed marijuana businesses

A SAR will be filed no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing the report. If no suspect was identified on the date of detection, the Bank may delay filing a SAR for an additional 30 calendar days to identify a suspect. In no case will the Bank delay the reporting for more than 60 calendar days after the date of initial detection of a reportable transaction. The Bank will notify the U.S. Attorney's Financial Task Force, by telephone, in situations involving violations requiring immediate attention, such as when a reportable violation is ongoing. The BSA/AML Officer will promptly notify the Board of Directors of any SARs filed. If a Board member is the subject of suspicious activity, the BSA/AML Officer will contact the other board members and ensure the confidentiality of the SAR filing.

The BSA/AML Officer will set up a file to document any conversations with law enforcement officials and note other pertinent facts concerning the transaction(s) and subsequent investigation. Copies of all SARs filed and supporting documentation will be retained for five years from the date of the filing. All supporting documentation must be made available to appropriate authorities upon request.

While considering the facts of the situation, the BSA/AML Officer may seek legal advice, as well as advice from the U.S. Attorney regarding possible "hold harmless" issues. The BSA/AML Officer will monitor the account activity for accounts that remain open after the filing of the SAR. If the suspicious activity continues, the Bank will re-file a SAR every 90 days until the activity stops, the account is closed, or further investigation provides a logical reason for this activity.

Activity That Is Not Reported On a SAR
If the decision is made not to file a SAR, after evaluating reported suspect activity and/or the review of accounts that are the subject of a subpoena or search warrant, the investigation should be documented and retained by the BSA/AML Officer. The documentation should include a recap of the information reviewed and the reason why the decision was made not to file a SAR. This documentation will be retained by the BSA/AML Officer.

Prohibition of SAR Disclosure
SARs are confidential. By law, directors, officers, employees, and agents of the Bank are prohibited from notifying the person(s) who are the subject of a SAR that a SAR has been completed and/or filed with FinCEN or other law enforcement agency.

Any employee who receives an inquiry or subpoena for information relating to or if they are requested to confirm a SAR has been filed, will decline from producing the SAR and/or any information that would disclose a SAR was been prepared or filed. All such inquiries are to be reported to the BSA/AML Officer immediately. The BSA/AML Officer will provide guidance to the employee and contact FinCEN and the FDIC regarding the request.

Safe Harbor for Banks from Civil Liability for Suspicious Activity Reporting
Federal law provides protection to the Bank from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether the reports are filed pursuant to SAR instructions. The law provides the Bank and its directors, officers, employees, and agents with a way to report suspicious activity to appropriate authorities in regards to any possible

violation of law or regulation. Specifically, it provides the Bank and its directors, officers, employees, and agents, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulations of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." This safe harbor applies to SARs filed within the required reporting thresholds, as well as SARs filed voluntarily on any activity below the thresholds.

Law Enforcement Inquiries and Requests
Law enforcement inquiries and requests can include grand jury subpoenas, National Security Letters (NSLs), and section 314(a) requests. Receipt of any law enforcement inquiry, does not, by itself, require the filing of a SAR by the bank. Nonetheless, any law enforcement inquiry will be reviewed by the SAR Committee.

National Security Letters (NSLs) – NSLs are written investigative demands that may be issued by the local Federal Bureau of Investigations (FBI) and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following: 1) Telephone and electronic communications records from telephone companies and Internet service providers; 2) Information from credit bureaus; and 3) Financial records from financial institutions.

NSLs are highly confidential documents; as such, examiners will not review or sample specific NSLs. Pursuant to 12 USC 3414(a)(3) and (5)(D), no bank, or officer, employee or agent of the institution, can disclose to any person that a government authority of the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL. The SAR Committee is to maintain the confidentiality of any law enforcement inquiry.

If the Bank files a SAR after receiving a NSL, the SAR will not contain any reference to the receipt or existence of the NSL.

The BSA/AML Officer will set up a file to document any conversations with law enforcement officials and note other pertinent facts concerning the transaction(s) and subsequent investigation. All files established as a result of receiving a request from law enforcement will be maintained by the BSA/AML Officer and care will be taken to ensure the confidentiality of the investigation.

Record Retention
The Bank will retain copies of SARs and supporting documentation for five years from the date of the SAR.

Large Currency Transaction Reporting

Reporting Requirements
The BSA requires the Bank to report all domestic currency transactions exceeding $10,000. The Bank must file a report of each deposit, withdrawal, exchange of currency, loan payment, or other transfer that involves a "transaction in currency" of more than $10,000. Some types of currency transactions need not be reported, such as those involving "exempt" persons. See the Exemption section of these procedures for more information.

Reportable Currency Transactions
Currency transactions that require the filing of a CTR include (but are not limited to):

- Cash deposits, cash withdrawals, or cashed checks.
- Investment deposits, time certificate deposits cashed or purchased with cash.
- Personal money orders, cashier's checks, traveler's checks, or official checks cashed or purchased with cash.
- Savings bonds cashed or purchased with cash.
- Corporate, registered, or bearer bonds cashed, including cashing coupons.
- Loans disbursed or collected in cash, including the payment of loan fees.
- Cash loan payments, loan proceeds.
- Securities sold or purchased in cash, including discount brokerage transactions.
- Cash exchanged for different denominations.
- Wire transfers that result in either a cash-in or cash-out.

Multiple transactions are aggregated and reported as a single transaction if the Bank has knowledge that the transactions are by, or on behalf of, one person, and the one business day total of the transactions is over $10,000. To determine the aggregate transactions, the following factors are used.

- Currency deposits made at a depository drop at night, over a weekend, or during a holiday are considered to be made on the banking day following the deposit.
- A business day is the day on which transactions are routinely posted to a customer's account.
- All currency transactions conducted from all branches are aggregated to determine the transaction amount.
- ATM transactions.

If an individual conducts a transaction on his/her own behalf and on behalf of another person (e.g. joint account), Part 1 must be completed for each person. If the transaction is conducted by an individual on behalf of another individual not present, Item 14 (“Method used to verify identity”) should be shown as NA. This applies to both deposits and withdrawals.

Currency
The definition of currency includes the coin and currency of the U.S. including U.S. silver certificates, U.S. notes, and Federal Reserve notes. The definition of currency also includes any country's circulated coin and currency that is used and accepted as money in the country of issue.

The definition of currency does not include bank checks or other negotiable instruments not customarily accepted as cash.

Reporting Procedures
When presented with a reportable transaction, a CTR will be completed. Any aggregate cash transaction over $3,000 will prompt a CTR information collection screen in the Bank’s core teller system at the time of transaction. After the core system hard posts transactions at end of day processing, data files are processed by the Bank’s BSA/AML software and generates CTRs for review. The BSA Analyst verifies the reports and checks daily aggregate reports to ensure the amounts reported are accurate. The CTR is then completed through the BSA/AML software and submitted to FinCEN via the BSA E-Filing System. Transaction must be reported within 15 calendar days from the transaction date. The Bank Secrecy Act Officer, or her designee, completes periodic reviews of CTRs to ensure accurate and timely reports are filed.

Filing Reports

The Bank Secrecy Act Analyst will review all CTRs for accuracy and queue them from submission to FinCEN. If the CTR is not properly completed, the BSA Analyst will review the errors and amend to ensure the necessary corrections are made in a timely manner.

The employee conducting the transaction will make every effort to gather appropriate information. The BSA Analyst will not delay filing the CTR if required information is missing. The incomplete CTR will be filed with an explanation. The BSA Department will prepare and file an amended CTR when the missing information is obtained.

Back-filing
The Bank makes every effort to identify and file all required CTRs. However, if the Bank has failed to file a CTR on multiple reportable transactions and the oversight is discovered, the Bank will begin to file CTRs on all reportable transactions and will contact FinCEN to request a determination on whether the back-filing of unreported transactions is necessary.

Record Retention
The Bank must maintain evidence of compliance with the Bank Secrecy Act for five (5) years from the date of each reported transaction or the occurrence of any act requiring documentation. **Appendix B** lists the types of records that must be retained for at least five (5) years.

The BSA Department will retain copies of all CTRs, correspondence, and other supporting documentation for five (5) years.

Correspondence with FinCEN
If FinCEN notifies the Bank that they have failed to supply FinCEN with critical information, or if they have failed to make appropriate corrections, the BSA Analyst will file an amended form. All responses to FinCEN will be made within 20 days of notification.

CMIR
Each person (including a bank) who physically transports, mails, or ships currency or monetary instruments in excess of $10,000 at one time into or out of the U.S. (and each person who causes such transportation, mailing, or shipment) must file a Report of International Transportation of Currency or Monetary Instruments ("CMIR"). The Bank is exempt from this reporting requirement when the currency is shipped overland via the Postal Service or common carrier. All other types of shipments, including air courier or via the airlines, require the completion of the CMIR. Regardless of whether an exemption from filing a CMIR applies, the Bank will monitor for, and report, suspicious activity involving the shipment of currency.

Additionally, and regardless of reporting requirements for the completion of a CMIR, the Bank is required to report all applicable cash transactions on a CTR even if the international transactions are subject to the exemption from filing a CMIR.

Timberland Bank does not transport currency or monetary instruments out of the U.S. If an instance arises where this may occur, the BSA/AML Officer will be contacted for guidance.

Exemptions

When the guidelines and regulations for completion of CTRs were written, FinCEN recognized that the routine reporting of some types of large currency transactions does not assist law enforcement

authorities and may place an unreasonable burden on the Bank. Therefore, the Bank may exempt certain types of customers from the currency transaction reporting requirements.

A two phase exemption process was established in 1994, when the Money Laundering Suppression Act ("MLSA") was written into law. Phase I exemptions apply to transactions in currency between banks, governmental departments or agencies, and public/listed companies and their subsidiaries. Phase II exemptions apply to businesses that meet specific criteria established by FinCEN. To exempt a customer from CTR reporting, the Bank will file a Designation of Exempt Person form.

Phase I Exemptions

FinCEN's rules identify five categories of Phase I exempt persons:

- Another bank in the U.S., to the extent of such banks domestic operations. This includes other domestic commercial banks, savings and loans, savings banks, and credit unions.
- A federal, state or local government (including the District of Columbia, U.S. territories and possessions and various tribal government authorities).
- Any entity that exercises government authority on behalf of the U.S. or any such state or political subdivision.
- Any entity (other than a bank) whose common stock is traded on the New York, American, or NASDAQ stock exchanges (with some exceptions).
- Any subsidiary (other than a bank) of any "listed entity" that is organized under U.S. law and at least 51 percent of whose common stock is owned by the listed entity.

A Designation of Exempt Person ("DEOP") is not required for any branch of the Federal Reserve Bank, other banks located within the United States, or government departments or agencies. The Bank will file a one-time Designation of Exempt Person form to exempt any other person identified as a Phase I entity. A Phase I exemption covers all transactions in currency with the exempted entity, not only transactions in currency conducted through an account. If required, the form will be filed with FinCEN within 30 days after the first transaction in currency that the Bank wishes to exempt.

Annual Review

The information supporting each designation of a Phase I exempt person will be reviewed and verified by the Bank at least once per year. However, annual reviews are not required for customers who are other banks or government agencies. All records for a Phase I exemption of a "listed entity" will contain, at least annually, a copy of the listing from the appropriate stock exchange, ensuring this documentation contains the date the listing was published. This will be accomplished through an Internet search or retaining a copy of the listing from a newspaper.

Phase II Exemptions

The second phase of the rule became effective October 21, 1998 and allows the Bank to exempt non-listed businesses and payroll customers. On January 5, 2009 the Phase II exemptions were modified once more. A business that does not fall into any of the Phase 1 categories may be exempted, if it qualifies as either a "non-listed business" or as a "payroll customer."

Non-listed Businesses

A non-listed business is an enterprise that, to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts, has: 1) maintained a transaction account at the bank for at least two months; 2) frequently engages (at least five times in a year) in transactions in currency in excess of $10,000; and 3) is incorporated or organized under the laws of the U.S., or is registered as and is eligible to do business in the U.S.

There are types of businesses which are not eligible for exemption under any circumstances. An ineligible business is a business engaged primarily in one or more of the following activities:

- Serving as a financial institution or as agents for financial institutions (for example, a Money Services Business) of any type.
- Purchasing or selling motor vehicles of any kind, vessels, aircraft, farm equipment, or mobile homes.
- Practicing law, accounting, or medicine.
- Auctioning of goods.
- Chartering or operation of ships, buses, or aircraft.
- Operating a pawn brokerage.
- Engaging in gaming of any kind (other than licensed pari-mutuel betting at race tracks).
- Engaging in investment advisory services or investment banking services.
- Engaging in any other activity that may, from time to time, be specified by FinCEN.
- Operating a real estate brokerage.
- Operating in title insurance activities and real estate closings.
- Engaging in trade union activities.
- Marijuana-related businesses

A business that engages in multiple business activities may qualify for an exemption as long as no more than 50% of its annual gross revenues are derived from one or more of the ineligible business activities. For example, a grocery store who sells lottery tickets may be eligible for exemption, as long as not more that 50% of its annual gross revenue comes from the lottery ticket sales. This documentation will include how the Bank determined that less than 50% of the annual gross revenues were from the ineligible activity. This determination may be based on the Bank's general understanding of the customer's business, the purpose of the customer account, and/or account activity reviews that demonstrate the majority of the business's activity is based on their primary business purpose.

Payroll Customers

A payroll customer is a person that: 1) has maintained a transaction account at the Bank for at least 12 months; 2) operates a firm that regularly withdraws more than $10,000 in order to pay its U.S. employees in currency; and 3) is incorporated or organized under the laws of the U.S., or is registered as and is eligible to do business in the U.S.

Initial Designation

When the Bank has determined that an entity is exempt for one of the above reasons, a Designation of Exempt Person form will be filed with FinCEN that identifies the exempt entity and the Bank. The Bank will file the Designation of Exempt Person within 30 days of the first customer transaction the Bank wishes to exempt. The BSA Officer will authorize the exempt status of all Bank customers. Of special consideration, in the event of the acquisition of another financial institution, the Bank must file a new initial Designation of Exempt Person form for each customer that the Bank determines qualifies for exemption post-acquisition. The new form must be filed in accordance with the normal initial designation timeline and procedures.

Annual Review

The information supporting the exemption of all Phase II businesses will be reviewed and verified at least once a year. Additionally, the Bank will establish and maintain a monitoring system that is reasonably designed to detect those transactions in currency that would require the Bank to file a Suspicious Transaction Report. The BSA Officer is responsible for the annual review of all Phase II exemptions.

Exemption list
The Bank will maintain a list of all exempt entities, along with a copy of the Designation of Exempt Person form(s) filed with FinCEN. These records will be maintained for five years.

Safe Harbor for Exemptions
The BSA provides a safe harbor to the Bank for the failure to file a CTR for a transaction in currency by an exempt person, unless the Bank knowingly provides false or incomplete information or has reason to believe that the customer does not qualify as an exempt customer. In the absence of any specific information that would alert the Bank to the fact the customer no longer meets the requirements of an exempt person, the Bank is entitled to safe harbor from civil penalties to the extent it continues to treat that customer as an exempt customer until the date of the customer's annual review.

Revoking an Exemption
The Bank can, for any reason, revoke the exemption status for a customer. Common reasons for revoking the exempt status of an account are a change in the ownership of the company, the company begins to engage in activities that now make it ineligible for exempt status, or account monitoring has indicated the currency transaction activity has changed without a known reason for the change – the account activity has become suspicious in nature. While it is not required, a Designation of Exempt Person form can be filed to notify FinCEN the exemption has been revoked. At a minimum, the Bank will document the date the exemption was revoked and indicate the exemption was revoked on the central list of exempt entities. The Bank will begin to file CTRs for this customer as of the date the exemption is revoked. The exemption records will be maintained for five years following the date the exemption was revoked.

Effect on Other Regulatory Requirements
The exemption procedures do not release the Bank from the requirement the Bank must file a SAR on a customer involved in suspicious account activity or any of the other recordkeeping requirements of the BSA/AML program. For example, the fact a customer is exempt from the filing of CTRs has no effect on the Bank's obligations to retain records of funds transfers by the customer or to retain records in connection with the sale of monetary instruments to that customer.

Cash Sale of Monetary Instruments
($3,000 Retention Rule)

Amendments to the Bank Secrecy Act require the Bank to obtain and maintain certain records regarding the cash purchase of cashier's checks, money orders, traveler's checks, and any other monetary instrument in amounts of $3,000 to $10,000. Purchase of monetary instruments under $10,000 is a common method used in money laundering schemes. Monetary instruments are easier to transport and negotiate than are large amounts of cash. The recordkeeping requirements differentiate between deposit account holders and non-deposit account holders/non-account holders. The Bank must obtain additional information from purchasers who do not have a deposit account with the bank. For example, additional information is required from someone whose only relationship with the bank is a mortgage loan or line of credit.

Transactions Covered by the $3,000 Rule
The $3,000 rule applies to each cash sale of bank checks or drafts, cashier's checks, money orders, traveler's checks, foreign drafts, prepaid access cards, and other similar monetary instruments.

The $3,000 rule is only triggered when cash is used to purchase a covered monetary instrument. The rule applies if the amount of the monetary instrument(s) is less than $3,000, but the service charge makes the "transaction in currency" $3,000 or more.

The $3,000 rule does not apply to purchases by check, other monetary instruments, or debits to accounts. The rule does not apply if the currency involved in the purchase of one or more monetary instruments by an individual exceeds $10,000. Instead, a CTR will be filed when the currency transaction exceeds $10,000.

Concurrent Multiple Purchases
The totals of concurrent multiple cash purchases of the same or different types of monetary instruments will be aggregated. Multiple purchases totaling between $3,000 and $10,000 will be treated as one purchase if the same Bank employee sells the monetary instruments at the same time or if the instruments are purchased during the same visit to the Bank.

This rule applies to the following examples of concurrent purchases:

- An individual uses cash to purchase two $1,500 Cashier's Checks while conducting other business with one teller.
- An individual uses cash to purchase a $1,500 Cashier's Check from one employee, then immediately uses cash to purchase $1,500 in traveler's checks from another employee.

This additional requirement is in the regulation to prevent money launderers from evading the identification requirements by buying numerous monetary instruments in amounts below $3,000 on the same business day at the same financial institution.

An individual Bank employee is thought to have knowledge of multiple purchases during any one business day under the following circumstances:

- The employee sells multiple monetary instruments to one purchaser.
- The employee observes an individual buying multiple monetary instruments during the same day.
- The employee is told by another employee that an individual purchased other monetary instruments.

- An individual informs an employee about multiple purchases.

Aggregation of Multiple Purchases
Multiple purchases will be aggregated and records retained if the Bank has knowledge that the transactions are by one person and the one business-day total of the purchases is between $3,000 and $10,000.

Interaction Between the $3,000 Rule and CTR Requirements
Certain situations require completing a CTR for purchases that are also covered by the $3,000 rule. This occurs when an individual conducts more than one type of cash-in transaction on the same day, totaling more than $10,000, and involving the purchase of one or more monetary instruments in amounts between $3,000 and $10,000.

The following example illustrates when both the CTR and the $3,000 rules are triggered:

- An individual makes a $5,000 cash deposit to a checking account. At the same time, the person uses cash to purchase a $7,000 Cashier's Check. A CTR will be completed for the $12,000 and required information retained regarding the purchase of the $7,000 Cashier's Check.

Purchases Requiring a CTR Only
When an individual uses cash to purchase a single monetary instrument in an amount exceeding $10,000, only the CTR rules apply. The same is true for concurrent and multiple cash purchases that total more than $10,000.

The following are examples of purchases not covered by the $3,000 rule: (required CTR only)

- An individual uses cash to purchase one $12,000 cashier's check.
- The Bank has knowledge of an individual's cash purchase of five cashier's checks in equal amounts of $2,900 during one business day ($14,500 aggregate).
- An individual uses cash to purchase a $5,000 cashier's check and $9,000 in traveler's checks.

As all of the currency transactions are of the same type (cash-ins to purchase one or more monetary instrument) and exceed $10,000, the Bank will file a CTR for the total amount of the currency transactions. The Bank is not required to retain information regarding the $3,000 rule.

Identification Requirements
The requirements for the cash sale of monetary instruments rules differentiate between purchasers who are deposit accountholders and purchasers who do not have a deposit account with the Bank.

An accountholder is anyone with a Timberland Bank checking account, savings account, time deposit, or money market account. If it cannot be verified that the purchaser is a deposit accountholder, that person will be treated as a non-accountholder for the purposes of retaining the required information.

A non-accountholder is a person who does not have a Timberland Bank checking account, savings account, time deposit, or money market account. Loan customers who do not maintain a deposit account will be treated as non-accountholders for the purposes of retaining the required information.

Before issuing a monetary instrument, the identity and address of the purchaser will be verified.

If the purchaser is a non-accountholder, the Bank must determine if the purchaser is acting on behalf of another person. If the purchase is on behalf of another person, identification for the third party will be obtained. See the Bank's Customer Identification Program procedures for identification information.

If the purchaser of a monetary instrument has a deposit account with the Bank, the following information will be obtained and retained:

- The name of the purchaser.
- The date of purchase.
- The type of instrument(s) purchased.
- The serial numbers of each instrument purchased.
- The dollar amount(s) of the instrument(s) purchased.
- The deposit account number of the purchaser.

If the purchaser of a monetary instrument does not have a deposit account with the Bank and an officer has approved the transaction, the following **additional** information will be obtained and retained.

- The physical address of purchaser.
- The Social Security number or alien identification number of the purchaser.
- The date of birth of the purchaser.
- The identifying information from the identification presented by the purchaser. (For example, the state of issuance and number from a driver's license.)

Refusal to Complete Sale

The Bank will verify the identity of the purchaser and retain the required information. The Bank will refuse to sell monetary instruments in amounts of $3,000 or more if the purchaser fails to provide the required information.

An exception to this strict rule may be made for a purchaser who has a legitimate reason for failing to provide identification containing their name and address. An example is someone who is elderly or disabled. In these circumstances, the Bank may accept a Social Security card or Medicare/Medicaid card along with another form of documentation bearing the customer's name and address. Additional forms of documentation include a utility bill, a tax bill, or a voter registration card.

Record Retention

The Bank will retain the required information for five years from the date of each reported transaction. This information must be accessible upon request by the Treasury.

A monetary instrument log is maintained in each branch.

Penalties for Noncompliance

The Bank may rely on the identification presented by the purchaser, unless the Bank has reason to believe or suspects that the identification may be false. If this occurs, the Bank will investigate further to determine if the purchaser is trying to launder money or is attempting to defraud the Bank.

If a Bank officer or employee suspects a customer is attempting to circumvent the reporting requirements of the BSA, but fails to investigate further or fails to report the suspicions to law enforcement, the Bank and the employee may be liable for being "willfully blind."

Funds Transfers

General

Under the Funds Transfer Recordkeeping rule, effective May 28, 1996, the Bank is required to collect, retain, and transmit information concerning payment orders and transmittal orders of $3,000 or more. These requirements are based on Bank's role in each funds transfer (originator, intermediary, or beneficiary). Covered payment and transmittal orders include those made by letter or other written communication, oral communication (including, but not limited to telephonic), or electronic communications.

Effective September 18, 2009, international ACH transactions must comply with the funds transfer travel rules. All international ACH transactions, regardless of the dollar amount, must comply with these rules. Additionally, the originating depository financial institutions must identify a cross-border ACH transaction with the Standard Entry Class code of "IAT" (International ACH Transaction). These changes in the ACH rules will provide information about inbound cross-border ACH transactions that will ensure the transactions are screened through OFAC and will identify them for use in determining any anti-money laundering risks.

These rules apply to inbound (originating outside of the United States) and outbound (from the United States to a foreign country) transactions. The IAT rules increased the amount of originator and beneficiary data available to the Bank, which will assist in the screening for OFAC and suspicious transactions. To help mitigate the risks presented by IAT transactions, the Bank will review each transaction separately (not as a batched transaction). This review can be manual or automated.

Telephonic or electronic instructions from a customer to transfer money may qualify as funds transfers for which the required information must be captured and retained. For instance, the following transactions are covered:

- A telephonic transfer of $3,000 or more from a business account to another company's account.
- A telephonic transfer of $3,000 or more from a business account to a consumer's account or a consumer's account to a business account.

Exempt Transactions

All funds transfers under $3,000 are exempt from the Funds Transfer Recordkeeping rules. Furthermore, all transfers governed by the Electronic Fund Transfers Act ("EFTA") as well as any other funds transfers that are made through an automated clearinghouse, ATM, or POS systems are exempt from these rules. The following funds transfers and transmittals of funds are also exempt from the recordkeeping requirements:

- Where both the originator and beneficiary, or the transmitter and the recipient, are any of the following:
    - A domestic bank.
    - A wholly owned domestic subsidiary of a bank chartered in the U.S.
    - A domestic broker or dealer in securities.
    - A wholly owned domestic subsidiary of a domestic broker or dealer in securities.
    - The United States.
    - A state or local government.
    - A federal, state, or local government agency or instrumentality.
- Where both the originator and beneficiary are the same and the same bank is used for the transaction.

- Where both the transmitter and recipient are the same and their financial institution is the same domestic broker or dealer in securities.

Responsibility of Originating Bank
When the Bank is the originating bank, which is the bank to which the sender issues the first payment order in a funds transfer, the following information will be obtained and retained for each payment order of $3,000 or more:

- The name and address of the originator.
- The account number of the originator.
- The amount of the payment order.
- The execution date of the payment order.
- Any payment instructions received from the originator with the payment order.
- The identity of the beneficiary's bank.
- As many of the following items as are received with the payment order:
    - The name and address of the beneficiary.
    - The account number of the beneficiary.
    - Any other specific identifier of the beneficiary (for example, CHIPS universal identifier, stock exchange identifier, Dun & Bradstreet identifier)

Additionally, the originating bank must identify all outgoing international ACH transactions with the new Standard Entry Class code of "IAT" and comply with the travel rule requirements for all outgoing international ACH transactions, regardless of the dollar amount involved.

It is the policy of Timberland Bank to collect and maintain all of the required information before completing a wire transfer. All wires, outgoing and incoming, must be checked against the OFAC control list prior to completing the request for a wire transfer. All foreign wires must be approved by the approved employees listed in the Wire Transfer Policy prior to completion of the wire transfer.

The Funds Transfer Recordkeeping rules define an established customer as "a person with an account with the Bank or a person with respect to which the Bank has obtained and maintains the name and address, as well as the customer's taxpayer identification number, or if none, alien identification number or passport number and country of issuance, and to which the Bank provides financial services relying on the information. These relationships with the Bank include deposit accounts, loan agreements, trust accounts, custody accounts, and mutual fund accounts."

It is the policy of Timberland Bank to only initiate or accept wires for established customers of the Bank. An exception to the policy will only be granted should the wire request be approved by Michael Sand or Jonathan Fischer. If an exception is granted, the non-established customer procedures will be followed. The BSA Officer will be notified and will log the exception.

Retrievability
The information retained by the Bank when originating a funds transfer must be retrievable by reference to the name of the originator and the account number. These records will be maintained for five years.

Non-Customer Wire Transfers

If the Bank accepts or initiates a wire transfer for a non-customer, management approval must be obtained prior to completing the transaction. A Pay Upon Proper Identification (PUPID) transaction poses a higher level of risk to the Bank.

Prior to releasing the funds from a PUPID transaction, the following identification must be obtained and retained with the wire transfer records:

- The full name of the person sending/receiving the wire.
- The address of the person sending/receiving the wire.
- Their Social Security number or alien identification number.
- Their date of birth.
- The identifying information from the identification presented. (For example, the state of issuance and number from a driver's license.)

To further reduce the risk presented by PUPID transactions, if an exception to policy is granted, the Bank will not send or receive a wire transfer for a non-customer over $5,000.

Prior to processing the wire transfer, the Treasurer or Assistant Treasurer will review and approve the transaction. OFAC screening will be performed and documented on all PUPID transactions prior to sending or releasing the funds. All PUPID transactions involving international wire transfers should be reported to the BSA/AML Officer. Additionally, any suspicious transactions involving a PUPID transaction will be reported to the BSA/AML Officer.

It is Bank policy not to send or receive wire transfers for non-customers.

Responsibilities of Intermediary Banks

If the Bank is acting as an intermediary for funds transfers/transmittals of $3,000 or more, the Bank will retain a record of the payment order.

Travel Rule Requirement

For funds transmittals of $3,000 or more, the Bank will include the following information, if received from the sender, in a transmittal order at the time the transmittal order is sent to a receiving financial institution:

- The name and address of the transmittor.
- The account number of the transmittor.
- The amount of the transmittal order.
- The date of the transmittal order.
- The identity of the recipient's financial institution.
- As many of the following items as are received with the transmittal order:
    - The name and address of the recipient.
    - The account number of the recipient.
    - Any other specific identifier of the recipient.
- Either the name and address or the numerical identifier of the Bank.

As an intermediary, the Bank will pass on all of the information received from a transmittor's financial institution or the preceding financial institution, but it does not have a duty to obtain information not provided by the transmittor's financial institution or the preceding financial institution.

Responsibilities of Beneficiary Banks
If the Bank receives a payment order of $3,000 or more as the beneficiary's Bank, the Bank will retain a copy of the payment order.

When the wire proceeds are disbursed to a beneficiary who is not an established customer of the Bank, we will verify the identity of the person receiving the funds. The following information will be obtained and a record of each item will be maintained:

- The beneficiary's name and street address;
- The type of identification reviewed;
- The number of the identification document (for example, the driver's license number); and
- The beneficiary's taxpayer identification number; or if none, the alien identification number, passport number – and country of issuance, or notes in the documentation to support the lack of a taxpayer identification number.

Retrievability
The information retained by the Bank when receiving a funds transfer must be retrievable by reference to the name of the beneficiary and the account number. These records will be maintained for five years.

There are no Travel Rule requirements for beneficiary banks.

USA PATRIOT Act

General
The USA PATRIOT Act ("Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act) was signed into law on October 26, 2001. The Act includes numerous provisions for fighting international money laundering and blocking terrorist access to the United States' financial system. The major components of the Act are discussed below.

Section 326, Customer Identification Program
Section 326 sets minimum standards for the identification of a customer in connection with the opening of an account at a financial institution. Information regarding that section is located in the Banks' Board approved Customer Identification Program ("CIP").

Section 311, Special Measures
Section 311 allows Treasury to impose special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, or types of accounts of primary money laundering concern. Treasury can require any of these five special measures, either individually, jointly, or in any combination:

- **Recordkeeping and Reporting of Certain Financial Transactions:** Banks may be required to maintain or to file reports concerning the aggregate amount of transactions or the specific of each transaction with respect to a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern.
- **Information Relating to Beneficial Ownership:** Banks may be required to take reasonable and practicable steps, as determined by the Secretary of the Treasury, to obtain and retain information concerning the beneficial ownership of any account opened or maintained in the U.S. by a foreign person (other than a foreign entity whose shares are subject to public reporting requirements or are listed and traded on a regulated exchange or trading market), or a representative of such foreign person, that involves a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern.
- **Information Relating to Certain Payable Through Accounts:** Banks that open or maintain a payable through account involving a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern, may be required to: 1) identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and 2) obtain information about each such customer (and representative) that is substantially comparable to that which a US depository institution obtains in the ordinary course of business with respect to its customers residing in the U.S.
- **Information Relating to Certain Correspondent Account:** Banks that open or maintain a correspondent account in the U.S. involving a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern may be required to: 1) identify each customer (and representative) who is permitted to use the account or whose transactions are routed through the account; and 2) obtain information about each such customer (and representative) that is substantially comparable to that which a U.S. depository institution obtains in the ordinary course of business with respect to its customers residing in the U.S.
- **Prohibitions or Conditions on Opening or Maintaining Certain Correspondent or Payable Through Accounts:** Banks may be prohibited from opening or maintaining any

correspondent account or a payable-through account for, or on behalf of, a foreign financial institution if the account involves a jurisdiction, financial institution, class of transactions, or type of account that is of primary money laundering concern. This imposition of this measure can prohibit U.S. banks from establishing, maintaining, administering, or managing a correspondent or payable through account for, or on behalf of, any financial institution from a specific foreign jurisdiction. This measure may also be applied to specific foreign financial institutions and their subsidiaries.

The regulations that implement these prohibitions may require banks to review their account records to determine that they maintain no accounts directly from, or on behalf of, such entities. In addition to the direct prohibition, banks may also be:

- Prohibited from knowingly providing indirect access to the specific entities through its other banking relationships.
- Required to notify correspondent accountholders that they must not provide the specific entity with access to the account maintained at the U.S. bank.
- Required to take reasonable steps to identify any indirect use of its accounts by the specific entity.

Orders and regulations implementing specific special measures taken under section 311 are not static; they can be issued or rescinded over time as the Secretary of the Treasury determines that a subject jurisdiction, institution, class of transactions, or type of account is no longer of primary money laundering concern. Additionally, special measures imposed against one jurisdiction, institution, class of transactions, or type of account may vary from those imposed in other situations.

By policy, Timberland Bank does not maintain accounts directly from, or on behalf of, a foreign jurisdiction or a foreign financial institution. If an existing account is located that fits this description, the Bank will immediately complete the steps necessary to close the account at the earliest possible date.

Section 312, Private Banking and Account for Foreign Financial Institutions

Section 312 requires each U.S. financial institution that establishes, maintains, administers or manages a correspondent account in the United States for a foreign financial institution to establish "appropriate, specific and where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to enable the Bank to detect and report, on an on-going basis, any known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, or managed by the bank in the United States for a foreign financial institution (foreign correspondent account.) All accounts for foreign financial institutions are subject to due diligence and, based on the Bank's risk assessment of the account, may be subject to enhanced due diligence.

If the Bank is not able to perform due diligence at account opening, they will refuse to open the account. If an account is opened and is later identified as an account held by a foreign financial institution, the Bank will suspend transaction activity until due diligence can be performed. If due diligence cannot be performed, the account will be closed and a SAR will be filed.

Section 312 also requires each U.S. financial institution that establishes, maintains, administers or manages a private banking account in the United States for a non-U.S. person to establish "appropriate, specific and where necessary, enhanced due diligence policies, procedures, and controls that are reasonably designed to enable the Bank to detect and report instances of money laundering" through

those accounts. (Note: These requirements apply to ALL correspondent and private banking accounts for non-U.S. persons, regardless of when they were opened.)

- A "private banking" account is an account or combination of accounts that:
  - Requires a minimum aggregate deposit of U.S. $1,000,000 – Note: May apply if under the minimum if it appears the bank may be circumventing requirements by opening for just under the threshold.
  - Is established on behalf of one or more individuals who have a direct or beneficial ownership in the account.
  - Is assigned to, or administered or managed (in whole or part) by an officer, employee, or agent of a financial institution acting as a liaison between the financial institution and the direct and beneficial owner of the account.
- Minimum standards for non-U.S. persons
  - Determine the identity of the nominal and beneficial owners of the funds.
  - Conduct enhanced scrutiny of any private banking account that is requested or maintained by, or on behalf of, a senior foreign political figure, or any immediate family member or close associate of a senior foreign political figure (also known as politically exposed persons (PEPs). This enhanced scrutiny is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.
  - Determine the source of funds deposited into the private banking account(s). This includes determining the nature of the private banking customer's business, the source of the customer's wealth, and the extent to which the customer's business history presents an increased risk for money laundering.
  - Determine the size, purpose, and type of account(s) involved in the banking relationship and the anticipated activity of the account – dollar amount, number, and types of transactions.
  - Determine the nature and duration of the bank's relationship with the private banking customer.
  - Determine the private banking customer's home and business location(s). This must include considering the extent to which these locations are internationally recognized as presenting a greater risk for money laundering or, conversely, if it is considered to have acceptable AML standards.
  - Determine any information known or reasonably available to the Bank about the private banking customer. The scope and depth of this research will depend on the nature of the information that is available for review.

By policy, Timberland Bank does not maintain correspondent accounts for foreign financial institutions or private banking accounts for foreign persons, as defined in the USA PATRIOT Act.

By policy, Timberland Bank does not maintain private banking accounts, as defined in Section 312 of the USA PATRIOT Act.

Sections 313 and 319(b) include the following requirements. These regulations relate to foreign correspondent accounts.

For the purposes of these regulations, a "correspondent" account is an account established by a bank for a foreign bank to receive deposits from, to make payments or other disbursements on behalf of a foreign bank, or to handle other financial transactions related to the foreign bank. An "account" means any

formal banking or business relationship established to provide regular services, dealings, and other financial transactions. It includes a demand deposit, savings deposit, or other transaction or asset account, and a credit account or other extension of credit.

Section 313, Accounts for Foreign Shell Banks

Section 313 prohibits the Bank from establishing, maintaining, administering, or managing a correspondent account in the U.S. for, or on behalf of, a foreign shell bank. A foreign shell bank is defined as a foreign bank without a physical presence in any country. There is one exception that permits a bank to maintain a correspondent account for a foreign shell bank that is a regulated affiliate. Section 313 also requires that a bank take reasonable steps to ensure that a correspondent account for a foreign bank is not being used to provide banking services indirectly to foreign shell banks.

Certifications**:** A bank that maintains a correspondent account in the U.S. for a foreign bank must maintain records in the U.S. identifying the owners of each foreign bank. (Ownership information is not required for foreign financial institutions that file a form FR Y-7 – Annual Report of Foreign Banking Organizations.) A bank must also record the name and street address of a person who resides in the U.S. and who is authorized, and has agreed, to be an agent to accept service of legal process. The Bank will produce these records within seven days upon receipt of a written request from a federal law enforcement officer.

The U.S. Treasury has developed a certification process to assist banks in complying with the recordkeeping provisions.

- For a bank to have safe harbor from liability for failing to comply with the regulation, the bank may use a "Certification Regarding Correspondent Accounts for Foreign Banks" form. The form must be:
    - Obtained once every three years (using a "Recertification Regarding Correspondent Accounts for Foreign Banks" form).
    - Retained by the Bank for five years after the account is closed.
    - Requires banks to terminate correspondent accounts of foreign banks if they fail to comply with a request from the Secretary of Treasury or Attorney General of the U.S.

If, within 30 calendar days, the Bank is not able to obtain the required information, the Bank must close accounts for, and cease transactions with this foreign bank.

Section 319(b), Subpoenas/Summons on Accounts for Foreign Financial Institutions

Under section 319(b) of the Patriot Act, the Secretary of the Treasury or the U.S. Attorney General may issue a subpoena or summons to any foreign bank that maintains a correspondent account in the U.S. to obtain records relating to that account, including records retained outside of the U.S. If the foreign bank fails to comply with the subpoena or fails to initiate proceedings to contest the subpoena, the Secretary of the Treasury or the U.S. Attorney General may, by written notice, direct the Bank to terminate its relationship with a foreign correspondent bank. The Bank will comply with this notice within 10 days of receipt of the notice. Failure to comply within this time frame subjects the Bank to the possibility of a civil money penalty of up to $10,000 per day until the correspondent relationship is terminated.

Additionally, this section:

- Requires the Bank to maintain records for five years after an account is closed.

- Requires the Bank to make available information and account documentation for an account maintained in the U.S. no later than 120 hours after receiving a request for information relating to its customer's anti-money laundering compliance from an appropriate banking agency.

By policy, Timberland Bank does not maintain foreign correspondent accounts. If an existing account is located that fits this description, the Bank will immediately complete the steps necessary to close the account at the earliest possible date.

Section 314, Information Sharing

Section 314 facilitates the exchange of information (1) between the government and financial institutions and (2) among financial institutions.

Section 314(a) - Information-sharing between the government and financial institutions

A federal law enforcement agency investigating terrorist activity or money laundering may submit a request to FinCEN asking FinCEN to ask financial institutions, or a group of financial institutions, for certain information. If the request is properly submitted, FinCEN will ask financial institutions to search their records to determine whether they maintain or have maintained accounts for or engaged in transactions with the specified individual, entity, or organization.

The Bank will search its records and respond to FinCEN, within 14 days of receipt of the request, if there are any possible matches. A negative response is not required. The only information the Bank will provide to FinCEN is the confirmation there is a possible match. No further action is required unless or until the Bank receives a formal request for further information.

These requests, unlike OFAC lists, are not "watch lists." The search is a onetime inquiry. There are no updates or corrections issued if an investigation is dropped, a prosecution is declined, or the subject is not determined to be a viable suspect. The names contained in the requests do not correspond to convicted or indicted persons; the law enforcement agency is only requesting assistance in locating additional information to allow them to make a determination about proceeding with a case or potential case.

The Bank is not required to file a SAR based solely on identifying a possible match to a 314(a) request. The Bank will refer all possible matches to the BSA/AML Officer for further investigation and to determine if a SAR should be filed.

The Bank must:

- Designate a contact person to receive information requests.
- Within 14 days of receiving the request, search its database(s) to determine if it maintains or has maintained accounts or engaged in transactions with individuals or entities listed in a request by FinCEN.
    - This record search must include current accounts, accounts opened in the prior 12 months and transactions conducted outside of an account in the preceding 6 months. These records include:
        - Any type of deposit account (including CDs or an account held in the Trust dept.) in the past 12 months.
        - Safe deposit box in the past 12 months.

        - Borrower on a loan in the past 12 months.
        - Cash sales of a monetary instrument in the past six months.
        - Funds transfer records for the past six months.
- Within 14 days of receiving the request, notify FinCEN if an account or transaction is identified.
- Limit use of information received in the 314(a) request by FinCEN to:
    - Reporting to FinCEN;
    - Determining whether to establish or maintain an account or engage in a transaction; or
    - Assist in BSA/AML compliance.
- The Bank will not disclose to any person, other than FinCEN, the FDIC, or the federal law enforcement agency on whose behalf FinCEN is requesting information, that FinCEN has requested or obtained information.
- The Bank will not share the 314(a) requests with any foreign office, branch, or affiliate (unless the request specifically states otherwise), and the lists cannot be shared with affiliates, or subsidiaries of bank holding companies, if they are not financial institutions.
- The Bank will protect the security and confidentiality of the 314(a) requests by not maintaining any copies of the requests, either in paper or electronic form.

The BSA Officer is responsible for receiving the 314(a) requests from FinCEN. She, or her designee, will conduct the search within the established time limits and promptly report any matches to FinCEN.

Section 314(b) – This section provides the Bank with the ability to share information with other financial institutions and associations of financial institutions located in the U.S. in order to identify and report activities that may involve terrorist activity or money laundering. It also provides safe harbor provisions to the Bank as a protection from civil liability related to sharing this information.

To maintain protection under the safe harbor provisions, the Bank must:

- Notify FinCEN of its intention to share information, even when sharing with an affiliated financial institution.
    - This notice can be submitted electronically on http://www.treas.gov/fincen
    - The notice is effective for one year.
- Take reasonable steps to verify that, prior to sharing, the financial institution with which it intends to share information has submitted a notice to FinCEN.
- Limit the use of shared information to identifying and reporting on money laundering or terrorist activities, determining whether to establish or maintain an account or engage in a transaction, or assisting in complying with the BSA.
- Maintain adequate procedures to protect the security and confidentiality of the information.

Timberland Bank has filed a 314(b) Information Sharing notice with FinCEN. All communications with other financial institutions will be coordinated through and approved by the BSA Officer.

OFAC

Office of Foreign Assets Control

General

The Office of Foreign Assets Control ("OFAC") is an office of the Department of the Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security objectives against entities such as targeted foreign countries, terrorists, international narcotics traffickers, and those persons/governments engaged in activities related to the proliferation of weapons of mass destruction.

OFAC operates under Presidential wartime and national emergency powers, in addition to the authority granted to it by specific legislation. OFAC imposes controls on transactions or freezes assets under U.S. jurisdiction. Many of these sanctions are based on United Nations or other international mandates and they involve close cooperation with allied governments. Other sanctions are specific to the interests of the U.S. OFAC has been charged with the responsibility for promulgating, developing, and administering U.S. sanctions programs.

All U.S. persons, including U.S. Banks, bank holding companies, and non-bank subsidiaries must comply with OFAC regulations. All of the financial institution regulatory agencies cooperate in ensuring financial institution compliance with the OFAC Regulations. Unlike the BSA, the laws and regulations issued by OFAC apply not only to U.S. Banks, their domestic branches, agencies, and international banking facilities. The OFAC laws and regulations also apply to a bank's foreign branches and their overseas offices and subsidiaries.

In general, OFAC laws and regulations require the Bank to:

- Block accounts and other property of specified countries, entities, and individuals.
  Or
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.

The Bank must monitor all financial transactions performed, even when acting as an intermediary Bank, to detect those that involve any entity or person subject to the OFAC laws and regulations.

The BSA/AML Officer, who is also designated as the OFAC Compliance Officer, is responsible for monitoring and coordinating day-to-day compliance with the OFAC laws and regulations.

In most situations, the Bank will accept deposits and funds subject to OFAC regulations, but will immediately freeze the funds and accounts, so that absolutely no funds can be withdrawn (this is called "blocking"). The Bank will block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or through a blocked entity; or
- Are in connection with transactions in which a blocked individual or entity has an interest.

Occasionally, the Bank must reject the transaction or funds instead of accepting and blocking them. The Bank will receive notification from OFAC specific to rejecting the transaction at the time the OFAC screening is performed.

Exact regulations vary in accordance with requirements imposed by federal statute and the specific sanctions. A detailed description of specific regulations for each program is available on the official OFAC web site: www.treas.gov/ofac.

It should be noted that the OFAC prohibitions against certain countries, entities, and individuals are separate and distinct from the provisions within the USA PATRIOT Act that requires the Bank to compare accounts against government lists or 314(a) requests. OFAC lists have not been designated as government lists for the purposes of the Bank's Customer Identification Program.

Transactions Subject To OFAC

Every type of financial transaction will be reviewed for OFAC compliance including, without limitation, the following:

- Deposit accounts (checking, savings, etc.)
- Loans
- Lines of Credit
- Letters of Credit
- Safe Deposit boxes
- Wire Transfers
- ACH Transactions, including international ACH transactions
- Currency Exchanges
- Depositing or cashing checks
- Purchase of Money Orders or Cashiers Checks
- Loan Payments
- Guarantors and Collateral Owners
- Trust Accounts
- Prepaid access Cards, such as payroll cards, that fall within the CIP requirements
- Credit Cards
- Moreover, the names of all parties to a transaction must be checked against the list of names of individuals, entities, geographical locations, or countries that have been identified by OFAC. This includes, but is not limited to the following (as applicable):
  - Beneficiaries
  - Collateral Owners
  - Guarantors / Cosigners
  - Receiving Parties
  - Sending Parties

OFAC Screening Procedures

Timberland Bank runs OFAC scans on the entire customer database on a nightly basis. The Bank utilizes BSA/AML software to perform this service. Every new customer is screened at the time the relationship with the Bank is established.

Each transaction that involves a person or entity that is not a current customer will be individually checked against the OFAC SDN list prior to completion of the transaction. This includes wire transfers (both incoming and outgoing) and ACH transactions, including international ACH transactions. This screening is also performed through BSA/AML software.

The Bank uses Deluxe Detect consumer reports for new deposit accounts, a Kroll Factual Data credit report for new loan accounts, or a direct inquiry into the BSA/AML software to perform OFAC screening. All new deposit accounts, new safe deposit box holders, wire transfers, ACH transactions, and non-customer payees on official checks are screened prior to completing the transactions. Copies of the results of the screening are maintained in the BSA/AML software system. All new loan customers are screened prior to disbursement of any funds from a loan. The loan files contain a check list that includes confirmation the OFAC screening was performed.

If there is no match, the transaction may proceed. If there is a potential match, the Bank will perform additional due diligence to determine an actual or false positive match to the name on the OFAC list. If, through further research, it is determined the name is a false positive match, this will be documented and forwarded to the BSA/AML Officer. The BSA/AML Officer will maintain a file containing all of the false positive matches.

If the name is determined to be a true match, appropriate action must be taken to block (or reject, if applicable) the transaction:

- If the transaction is a deposit, the Bank will accept the transaction and immediately place the funds in a blocked account so no funds can be withdrawn. This will apply unless it is one of the few transactions that are to be rejected. If the transaction is to be rejected, the Bank will refuse to accept or proceed with the transaction.
- If the transaction is a transfer of funds (by, through or to Timberland Bank), the Bank is to accept the funds. Instead of completing the transfer, the funds will be placed in a blocked account so no funds can be withdrawn. If the transfer involves a transaction that is to be rejected, the Bank will refuse to accept or proceed with the transaction.

All accounts for the matched name will be frozen immediately. No funds can be withdrawn from any account(s) held in this name. In all cases, the BSA/AML Officer will be notified immediately. The BSA/AML Officer will ensure the funds are placed in an interest-bearing account from which only OFAC-authorized debits may be made. The BSA/AML Officer will file the appropriate report with OFAC within 10 days.

In general, the customer should be advised immediately of the blocking of the account or funds. The Bank may apply for a Specific License, which is filed with OFAC, if it wishes to try to facilitate the possible release of the blocked funds.

Demonstrating OFAC Compliance

Timberland Bank will maintain a list of all the false positive matches to help to identify other false positive matches in the future and to demonstrate that it is checking current customer lists and transactions for potential OFAC matches. The false positive list is maintained within the BSA/AML software.

Maintaining Current OFAC Lists

Within the BSA/AML software is an OFAC monitoring function. The OFAC list is updated within the system is updated immediately following the release of any OFAC change by the government. The BSA Department reviews the possible match list to ensure that none of the Bank's customers are on any of the government monitoring lists.

Specific Licensing

If the Bank would like OFAC to consider releasing funds that have been blocked; it is possible to apply for a Specific License. A Specific License is a written document issued by OFAC authorizing a particular transaction or set of transactions. The Bank must provide certain information including, without limitation, the following:

- Name of the blocked entity/account holder
- Amount of blocked funds
- Date of blocking
- Copies of documentation related to the underlying transaction
- Justification for the release of funds

Important OFAC Reports

There are a number of important reporting requirements for OFAC. The following three reports are critical:

1. Any transaction that has been blocked or rejected **must be reported to OFAC within ten calendar days** from the date the property became blocked (See OFAC Submission Report).
2. An annual report of all property blocked as of June 30 is due by September 30 of each year. (See Annual Report of Blocked Property).
3. OFAC requires the retention of all reports and blocked or rejected transaction records for five years.

Refer to **OFAC's website, http://www.treas.gov/offices/enforcement/ofac/,** for the OFAC Submission Reports and the Department of the Treasury's OFAC reporting documentation.

OFAC Submission Reports
Reports will be submitted to OFAC within ten calendar days for any transaction that has been blocked or rejected. The BSA/AML Officer will complete all OFAC submission reports. These reports will contain:

Blocked Transactions:

1. Timberland Bank's name and address (as holder of the account).
2. The name, title and phone number of the person that OFAC should contact for further information regarding the transaction or account.
3. Full information about the transaction including:
   - Full name of the owner or account party
   - A description of the property
   - The location of the property
   - Type of transaction, account or description of the property
   - Amount (actual or estimated)
   - Date of transaction
   - Date of report filing
   - Status and location of the account
   - Any information necessary
4. Confirmation that the property has been placed into a clearly identifiable, new or existing blocked account containing the name of (or interests of) the entity subject to blocking.
5. Name and phone number of the BSA/AML Officer.
6. A photocopy of any written instruction received concerning the transaction.

In addition to a submission report, Timberland Bank will submit photocopies of any applicable transfer/payment instructions, and confirmation that the funds are placed in a clearly marked account upholding the name/interests of the entity subject to blocking.

Rejected Transactions:

1. Timberland Bank's name and address (as holder of the account).
2. The name, title and phone number of the person that OFAC should contact for further information regarding the transaction or account.
3. Full information about the transaction including:
4. Name & address of the Transferee financial institution
5. Date of the transfer
6. Amount of the transfer
7. Basis for rejection
8. A photocopy of the payment and/or any transfer instructions received.
9. Name and phone number of the BSA/AML Officer at the Transferee institution.

Training

To ensure compliance, Timberland Bank will conduct OFAC training annually with the entire staff; in addition they will be given a copy of our OFAC procedures.

Penalties for Non-compliance

OFAC violations have serious consequences. Employees who fail to comply with the regulations may be subject to strong disciplinary action by the bank. Additionally, the individual(s) may face civil and criminal penalties, fines, and /or prison sentences. All employees are to read and be familiar with these procedures.

Remote Deposit Capture

The Bank may offer Remote Deposit Capture services to business customers who meet the criteria necessary to qualify for this service. Remote Deposit Capture ("RDC") allows a customer to convert checks received in the course of conducting their businesses to electronic images using a scanner. The images are then electronically transmitted to the Bank for processing. This allows the customer to make deposits without having to physically visit the Bank. Processing deposits in this manner reduces the cost and volume of paper associated with traditional methods of processing a deposit; such as face-to-face contact with a teller, night deposits, or mailing deposits to the Bank.

In addition to the benefits provided by this service, RDC may expose the Bank to various risks, including money laundering, fraud, and compromised transmission of financial data (information security). Controls must be put into place to mitigate these risks, reducing the exposure of the Bank to financial and reputation damages. Additionally, the Bank must monitor the RDC transmissions to identify possible money laundering and fraudulent transactions.

The Bank will develop the appropriate policies, procedures, and processes to mitigate the risks presented by RDC services. This will include:

- Developing a list of the types of businesses that are eligible for inclusion in the RDC program (or conversely, a list of the types of businesses that are not eligible). Higher risk customers may include online payment processors, credit repair services, some mail order or telephone order businesses, customers who offer online gambling services, offshore businesses, and adult entertainment businesses.
- Developing standard underwriting criteria for each customer who wishes to use the service.
- Setting appropriate maximums for large dollar items for each customer using the service.
- Obtaining the expected account activity from each customer using the service, such as the anticipated volume of checks that will be included in the transmissions, the dollar volumes, and the types of checks that will be included in the transmissions (personal, payroll, third-party, etc.).
- Establishing RDC contracts that require the customer to retain, protect, and ultimately destroy the original documents. This may include requirements that the RDC customer provide an original document (if it has not already been destroyed) to the Bank when it is needed to facilitate an investigation, provide a better image when a transmission is not clear, or to resolve disputes.
- Ensuring additional reviews are performed when significant changes occur in the type or volume of transmissions or in the underwriting criteria the Bank relied on when establishing the RDC services.
- Ensuring the RDC customers properly secure RDC equipment and that they have established procedures to prevent inappropriate use, including establishing effective equipment security controls, for example passwords and dual control access.
- Ensuring the RDC transmission data is included in the BSA/AML monitoring for suspicious or unusual transactions.

Prepaid Access Cards

There are many types of prepaid access, or stored value, card products the Bank may offer to our customers. The type of cards offered will determine the level of money laundering risk or other risks that the Bank must consider. If the cards are "branded" with the Bank's name and/or logo, there are additional responsibilities to consider.

There are two types of prepaid access cards – reloadable and non-reloadable:

- Non-reloadable cards do not establish a continuing relationship with the purchaser and are not subject to any type of customer identification requirements. However, all cash purchases of these cards should be reviewed to detect any suspicious activity or potential money laundering activity. An example of a non-reloadable card may be a travel card issued instead of traveler's checks or a small value gift card.
- Re-loadable cards may establish an on-going relationship with the purchaser. Examples of reloadable cards are payroll cards, some telephone calling cards, or pre-paid debit cards where the consumer can choose to add additional value to the card. A customer relationship is not established if the card is not branded with the Bank's name or logo or if the Bank is not going to be directly involved in servicing the card. An example of this type of a card is a generic VISA gift card offered as a convenience to Bank customers. If the cards are branded with the Bank's name or logo or if the Bank is also going to service the cards, similar to servicing an ATM or traditional debit card, a customer relationship may be established. If the Bank will periodically reload the cards, a customer relationship is established. Whenever an on-going customer relationship is established and the user is not already a customer of the Bank, each card holder must meet the identification requirements in the Bank's CIP.

If the Bank offers prepaid access cards that establish an on-going customer relationship, the Bank will develop the appropriate policies, procedures, and processes to mitigate the risks presented by the card. This will include:

- Obtaining and retaining identification, as set forth in the Bank's CIP.
- Conducting initial and on-going OFAC screening is performed on all card holders.
- Setting appropriate maximum dollar limits for the cards.
- Including the sale of the cards in the records kept for the cash sale of monetary instruments between $3,000 and $10,000.
- Ensuring the sale of these cards is monitored to ensure all CTR reporting requirements are met.
- Establishing procedures to detect suspicious activity that may indicate potential money laundering, the transport of numerous cards to locations outside of the United States, or other suspicious activity. All suspicious activity relating to the card will be reported to the BSA/AML Officer. The BSA/AML Officer will review the information and determine if a SAR should be filed.
- Establishing procedures for handling claims related to the issue of the prepaid access card. These claims include lost/stolen cards or unauthorized use of the cards. This may be included in the contract with the vendor that produces the card.
- Ensuring additional reviews are performed when significant changes occur in the type or volume of activity involving a prepaid access card. All suspicious activity relating to the card will be reported to the BSA/AML Officer. The BSA/AML Officer will review the information and determine if a SAR should be filed.

- Ensuring the prepaid access product(s) is included in the Bank's BSA/AML and OFAC Risk Assessments.
- Ensuring all the requirements of any contracts with the issuer of the cards are met. This may include providing information regarding the filing of a CTR, suspicious activity related to a card, or suspicious activity relating to the sale/maintenance of a group of cards.

At this time, the Bank does not offer prepaid access cards.

Marijuana-Related Businesses

The Controlled Substance Act ("CSA") makes it illegal under federal law to manufacture, distribute, or dispense marijuana. While federally illegal, many states have legalized certain marijuana-related activities. Washington State legalized the recreational use of marijuana in November 2012. In light of these developments, the US Department of Justice ("DOJ") Deputy Attorney James M. Cole provided updated guidance to federal prosecutors concerning marijuana enforcement under the CSA, popularly known as "The Cole Memo," on February 14, 2014. The Cole Memo guidance applied to all of DOJ's federal enforcement activity, including civil enforcement and criminal investigations and prosecutions, concerning marijuana in all states. Also on February 14, 2014, the Financial Crimes Enforcement Network ("FinCEN") issued guidance regarding the BSA/AML reporting responsibilities for institutions that choose to provide financial services to State-legal marijuana businesses. In January 2018, the DOJ rescinded all previously issued marijuana-related memos; however, FinCEN's guidance is considered to be valid and current guidance for the BSA/AML responsibilities relating to State-legal marijuana businesses. The key elements of concern stem back to, and reference, the eight priorities identified by Deputy Cole in the Cole Memo:

- Preventing the distribution of marijuana to minors;
- Preventing revenue from the sale of marijuana from going to criminal enterprises, gangs, and cartels;
- Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
- Preventing state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
- Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
- Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
- Preventing the growing of marijuana on public lands and the attendant public safety and environmental dangers posed by marijuana production on public lands; and
- Preventing marijuana possession or use on federal property

According to FinCEN's guidance, FIN-2014-G001, the obligation to file a SAR is unaffected by any state law that legalizes marijuana-related activity. A financial institution is required to file a SAR if, consistent with FinCEN regulations, the financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution: (i) involves funds derived from illegal activity or is an attempt to disguise funds derived from illegal activity; (ii) is designed to evade regulations promulgated under the BSA, or (iii) lacks a business or apparent lawful purpose. Because federal law prohibits the distribution and sale of marijuana, financial transactions involving a marijuana-related business would generally involve funds derived from illegal activity. Therefore, a financial institution is required to file a SAR on activity involving a marijuana-related business (including those duly licensed under state law), in accordance with this guidance and FinCEN's suspicious activity reporting requirements and related thresholds.

Marijuana-business related SARs must contain specific language in order to file reports that are highly useful to criminal investigations and proceedings, according to the following guidelines:

"Marijuana Limited" SAR Filings

A financial institution providing financial services to a marijuana-related business that it reasonably believes, based on its customer due diligence, does not implicate one of the Cole Memo priorities or violate state law should file a "Marijuana Limited" SAR. The content of this SAR should be limited to the following information: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) the fact that the filing institution is filing the SAR solely because the subject is engaged in a marijuana-related business; and (iv)the fact that no additional suspicious activity has been identified. Financial institutions should use the term "MARIJUANA LIMITED" in the narrative section.

A financial institution should follow FinCEN's existing guidance on the timing of filing continuing activity reports for the same activity initially reported on a "Marijuana Limited" SAR. The continuing activity report may contain the same limited content as the initial SAR, plus details about the amount of deposits, withdrawals, and transfers in the account since the last SAR. However, if, in the course of conducting customer due diligence (including ongoing monitoring for red flags), the financial institution detects changes in activity that potentially implicate one of the Cole Memo priorities or violate state law, the financial institution should file a "Marijuana Priority" SAR.

"Marijuana Priority" SAR Filings

A financial institution filing a SAR on a marijuana-related business that it reasonably believes, based on its customer due diligence, implicates one of the Cole Memo priorities or violates state law should file a "Marijuana Priority" SAR. The content of this SAR should include comprehensive detail in accordance with existing regulations and guidance. Details particularly relevant to law enforcement in this context include: (i) identifying information of the subject and related parties; (ii) addresses of the subject and related parties; (iii) details regarding the enforcement priorities the financial institution believes have been implicated; and (iv) dates, amounts, and other relevant details of financial transactions involved in the suspicious activity. Financial institutions should use the term "MARIJUANA PRIORITY" in the narrative section to help law enforcement distinguish these SARs.

"Marijuana Termination" SAR Filings

If a financial institution deems it necessary to terminate a relationship with a marijuana-related business in order to maintain an effective anti-money laundering compliance program, it should file a SAR and note in the narrative the basis for the termination. Financial institutions should use the term "MARIJUANA TERMINATION" in the narrative section. To the extent the financial institution becomes aware that the marijuana-related business seeks to move to a second financial institution, FinCEN urges the first institution to use Section 314(b) voluntary information sharing (if it qualifies) to alert the second financial institution of potential illegal activity.

Limitations on Marijuana-Related Business Accounts

The Bank has established robust procedures for complying with the spirit of the Cole Memo and FinCEN's Red Flags. The Bank has established two separate account types to contain all marijuana-related business accounts: one for licensed entities that directly "touch" the plant and one for entities that have an indirect relationship to the plant. Licensed entity accounts are prohibited from originating international wires, cannot obtain Merchant Services products, may not be exempt from CTR filing, and all account activities to be reviewed quarterly in order to facilitate the extreme enhanced due diligence

required by FinCEN. Non-licensed entities have slightly less stringent reporting procedures but are actively monitored through enhanced due diligence processes.

Timberland will not initiate a lending relationship directly with a licensed marijuana business. Additional due diligence may be required on commercial loans that lease or rent space to marijuana businesses; however, these indirect lending relationships are discouraged. The limit of total marijuana related deposit account balances are restricted to $65 million.

Please see the Marijuana Related Banking Program for complete details on the account opening, monitoring, and reporting process of each account type.

Appendix A

Red Flags for Suspicious Transactions

The following are examples of potentially suspicious activities. Sometimes these are referred to as "red flags." This list is not all inclusive. However, it may assist the Bank in recognizing money laundering and terrorist financing schemes.

If the described activity is encountered, additional investigation of the activity is needed to determine if the activity is, in fact, suspicious. All suspicious activity must be reported to the BSA/AML Officer immediately. The BSA/AML Officer will be responsible for determining if a SAR should be filed and will make decisions regarding the continued servicing of the account(s) involved.

Potentially Suspicious Activity That May Indicate Money Laundering

Insufficient or Suspicious Customer Information

- At the time a new account is established, a business is reluctant to provide complete information about the purpose of business, its prior banking relationships, names of its officers and directors, and information about the location of the business.
- A customer provides unusual or suspicious identification documents that cannot be verified through the usual methods.
- The customer's home or business telephone is disconnected.
- The customer's background is at variance with his or her business activities.
- A customer makes frequent or large transactions and has no record of past or present employment experience.
- A customer's refusal to provide the usual information necessary to qualify for credit or other banking services.
- A spike in the customer's account activity with little or no explanation.
- A customer desires to open an account without providing references, a local address, or identification (passport, alien registration card, driver's license, or social security card); or refuses to provide any other information the Bank requires to open an account.
- No record of past or present employment on a loan application.
- The customer's financial statements differ from those of similar businesses.

Activity Inconsistent with the Customer's Business

- The currency transaction patterns of a business experience a sudden and inconsistent change from normal activities.
- A customer's corporate account(s) has deposits or withdrawals primarily in cash rather than checks.
- The owner of both a retail business and a check cashing service does not ask for cash when depositing checks, possibly indicating the availability of another source of cash.
- The customer engages in unusual activity in cash purchases of traveler's checks, money orders, or cashier's checks.
- A large volume of cashier's checks, money orders, and/or funds transfers is deposited into, or purchased through, an account when the nature of the account holder's business would not appear to justify such activity.
- A customer frequently makes large dollar transactions (such as deposits, withdrawals, or purchases of monetary instruments) without an explanation as to how they will be used in the

business, or the purchases allegedly are for a business that generally does not deal in large amounts of cash.

- A business account history that shows little or no regular, periodic activity; the account appears to be used primarily as a temporary repository for funds that are transferred abroad. For example, numerous deposits of cash followed by lump-sum wire transfers.
- A customer's place of business or residence is outside the Bank's service area.
- A corporate customer who frequently makes large cash deposits and maintains high balances, but does not use other banking services.
- A retail business routinely makes numerous deposits of checks, but rarely makes cash withdrawals for daily operations.
- A retail business has dramatically different patterns of cash deposits from similar businesses in the same general location.
- The amount and frequency of cash deposits are inconsistent with that observed at the customer's place of business.
- The business frequently deposits large amounts of cash, but checks or other debits drawn against the account are inconsistent with the customer's retail business.
- Businesses that do not normally generate currency make numerous currency transactions (i.e., a sanitation company that makes numerous deposits of cash).
- Financial transactions involving monetary instruments that are incomplete or contain fictitious payees, remitters, etc., if known.
- Unusual transfer of funds among related accounts or accounts that involve the same principal or related principals.
- A business owner, such as an owner who has only one store, who makes several deposits the same day using different bank branches.

Avoiding the Reporting or Record Keeping Requirement

- A business or customer asks to be exempted from reporting or recordkeeping requirements.
- A customer intentionally withholds part of the currency deposit or withdrawal to keep the transaction under the reporting threshold.
- A customer is reluctant to provide the information needed to file a mandatory report, to have the report filed, or to proceed with a transaction after being informed that the report must be filed.
- A customer or group tries to persuade a bank employee not to file required reports or to not maintain required records.
- An automatic teller machine(s) (ATM) is used to make several bank deposits below a specified threshold.
- A customer is reluctant to furnish identification when purchasing monetary instruments in recordable amounts.
- A customer requests access to a safe deposit box after completing a transaction involving a large withdrawal of cash, or accesses the safe deposit box before making cash deposits at or just under $10,000, in an effort to evade CTR filing requirements.
- Deposits are structured through multiple branches or by multiple persons who enter the branch together.
- Cash is deposited or withdrawn in amounts just below identification or reporting thresholds.

Funds Transfers

- Funds transfer activity to/from financial secrecy haven countries, or a high-risk geographic location, without an apparent business reason or when it is inconsistent with the customer's business or history.
- Periodic wire transfers from a personal account(s) to bank secrecy haven countries.
- Large incoming funds transfer on behalf of a foreign client with little or no explicit reason for receiving the funds.
- Frequent or large volume of wire transfers to and from offshore banking centers.
- Frequent funds transfers in large, round dollar amounts.
- Funds transferred in and out of an account on the same day or within a relatively short period of time.
- Payments or receipts with no apparent links to legitimate contracts, goods, or services.
- Transfers routed through multiple foreign or domestic banks.
- Unexplained repetitive or unusual patterns of activity.
- Deposits of funds into several accounts, usually in amounts of less than $3,000, which are subsequently consolidated into one master account and transferred outside of the country.
- Instructions to the Bank to wire transfer funds abroad and to expect an incoming wire transfer of funds (in an equal amount) from other sources.
- Regular deposits or withdrawals of large amounts of cash, using wire transfers to, from, or through countries that either are known sources of narcotics or whose laws are ineffective in controlling the laundering of money.
- Many small incoming funds transfers are received or deposits made using checks and money orders. Almost immediately, all or most of the funds are wired or transferred to another city or country in a manner inconsistent with the customer's business or history.
- Large volume of wire transfers from persons or businesses that do not hold accounts.
- Funds transfers to or from the same person to or from different accounts.

Bank Employee Activities

- Lavish lifestyle cannot be supported by an employee's salary.
- Absence of conformity with recognized policies, procedures, and processes.
- Reluctance to take a vacation.

Bank to Bank Transactions

- Significant changes in currency shipment patterns between correspondent banks.
- Significant turnover in large denomination bills that would appear uncharacteristic given the bank's location.
- Inability to track the true account holder of correspondent or concentration account transactions.
- The rapid increase in the size and frequency of cash deposits with no corresponding increase in non-cash deposits.

Other Suspicious Activity

- Substantial deposit(s) of numerous $50 and $100 bills.
- Mailing address outside the United States.
- Frequent exchanges of small dollar denominations for large dollar denominations.
- Certificate(s) of deposit or other investment vehicle used as loan collateral.
- A large loan is suddenly paid down with no reasonable explanation of the source of funds.

- Frequent deposits of large amounts of currency wrapped in currency straps that have been stamped by other banks.
- Frequent deposits of cash wrapped in currency straps or cash wrapped in rubber bands that are disorganized and do not balance when counted.
- Frequent deposits of musty or extremely dirty bills.
- A customer who purchases cashier's checks, money orders, etc., with large amounts of cash.
- A professional service provider, such as a lawyer, accountant, or broker, who makes substantial deposits of cash into client accounts or in-house company accounts, such as trust accounts and escrow accounts.
- A customer insists on meeting bank personnel at a location other than their place of business.
- Domestic bank account opened in the name of a casa de cambio (money exchange house), followed by suspicious wire transfers and/or structured deposits (under a specified threshold) into these accounts.
- Suspicious movements of funds from one bank into another bank and back into the first bank. For example: 1) purchasing cashier's checks from bank A; 2) opening up a checking account at bank B; 3) depositing the cashier's checks into a checking account at bank B; and 4) wire transferring the funds from the checking account at bank B into an account at bank A.
- Offshore companies, especially those located in bank secrecy haven countries, asking for a loan from a domestic U.S. bank, or for a loan secured by obligations of offshore banks.
- Use of loan proceeds in a manner inconsistent with the stated loan purpose.
- A customer who purchases a number of cashier's checks, money orders, or traveler's checks for large amounts under a specified threshold, or without apparent reason.
- Couriers, rather than personal account customers, make the deposits into the account.
- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them.
- The customer visits a safe deposit box or uses a safe custody account on an unusually frequent basis.
- Safe deposit boxes or safe custody accounts opened by individuals who do not reside or work in the Bank's service area, although financial institutions are available closer to them.
- Unusual activity in the safe deposit box area or unusual use of safe custody accounts. For example, frequent entry or use, carrying bags or other containers that could conceal large amounts of cash, monetary instruments, or small valuable items.
- Renting multiple safe deposit boxes to park large amounts of cash, monetary instruments, or high-value assets awaiting conversions to cash, for placement into the banking system. Similarly, using multiple safe deposit boxes to park large amounts of securities awaiting sale and conversion to cash, monetary instruments, outgoing funds transfers, or a combination of these, for placement into the banking system.

Potentially Suspicious Activity That May Indicate Terrorist Financing

Activity Inconsistent with the Customer's Business

- Funds are generated by a business owned by persons of the same origin or by a business that involves persons of the same origin from high-risk countries. (For example, countries designated by national authorities and FATF as non-cooperative countries and territories.)
- The stated occupation of the customer is not commensurate with the type or level of account or cash activity.

- Persons involved in cash transactions share the same address or telephone number, particularly when the address is a business location or does not seem to correspond to the stated occupation (For example, a business address when the customer states they are unemployed.)
- Financial transactions for nonprofit or charitable organizations in which there is no apparent logical economic purpose or in which there does not appear to be a link between the stated activity of the organization and the other parties in the transaction.
- A safe deposit box opened on behalf of a commercial entity when the business activity of the customer is unknown or the business activity does not appear to justify the use of a safe deposit box.

Funds Transfers

- A large number of incoming or outgoing funds transfers through a business account and there appears to be no logical business or other economic purpose for the transfers, particularly when this activity involves high-risk locations.
- Funds transfers are requested in small amounts in an apparent effort to avoid triggering identification or reporting requirements.
- Funds transfers do not include information on the originator, or the person on whose behalf the transaction is conducted, when the inclusion of such information would be expected.
- Multiple personal and business accounts or the accounts of nonprofit organizations or charities are used to collect and funnel funds to a small number of foreign beneficiaries.
- Foreign exchange transactions are performed on behalf of a customer by a third party, followed by funds transfers to locations having no apparent business connection with the customer or to high-risk countries.

Other Transactions Linked to Areas of Concern

- Transactions involving foreign currency exchanges are followed within a short time by funds transfers to high-risk locations.
- Multiple accounts are used to collect and funnel funds to a small number of foreign beneficiaries, both persons and businesses, particularly in high-risk locations.
- A customer obtains a credit instrument or engages in commercial financial transactions involving the movement of funds to or from high-risk locations when there appears to be no logical business reasons for dealing with those locations,.
- Banks from high-risk locations open accounts.
- Funds are sent or received via international transfers from or to high-risk locations.
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge.

Red Flags to Distinguish Marijuana Priority SARs

- A customer appears to be using a state-licensed marijuana-related business as a front or pretext to launder money derived from other criminal activity (i.e., not related to marijuana) or derived from marijuana-related activity not permitted under state law. Relevant indicia could include:
  - The business receives substantially more revenue than may reasonably be expected given the relevant limitations imposed by the state in which it operates.
  - The business receives substantially more revenue than its local competitors or than might be expected given the population demographics.

- The business is depositing more cash than is commensurate with the amount of marijuana-related revenue it is reporting for federal and state tax purposes.
- The business is unable to demonstrate that its revenue is derived exclusively from the sale of marijuana in compliance with state law, as opposed to revenue derived from (i) the sale of other illicit drugs, (ii) the sale of marijuana not in compliance with state law, or (iii) other illegal activity.
- The business makes cash deposits or withdrawals over a short period of time that are excessive relative to local competitors or the expected activity of the business.
- Deposits apparently structured to avoid Currency Transaction Report ("CTR") requirements.
- Rapid movement of funds, such as cash deposits followed by immediate cash withdrawals.
- Deposits by third parties with no apparent connection to the accountholder.
- Excessive commingling of funds with the personal account of the business's owner(s) or manager(s), or with accounts of seemingly unrelated businesses.
- Individuals conducting transactions for the business appear to be acting on behalf of other, undisclosed parties of interest.
- Financial statements provided by the business to the financial institution are inconsistent with actual account activity.
- A surge in activity by third parties offering goods or services to marijuana-related businesses, such as equipment suppliers or shipping servicers.

- The business is unable to produce satisfactory documentation or evidence to demonstrate that it is duly licensed and operating consistently with state law.
- The business is unable to demonstrate the legitimate source of outside investments.
- A customer seeks to conceal or disguise involvement in marijuana-related business activity. For example, the customer may be using a business with a non-descript name (e.g., a "consulting," "holding," or "management" company) that purports to engage in commercial activity unrelated to marijuana, but is depositing cash that smells like marijuana.
- Review of publicly available sources and databases about the business, its owner(s), manager(s), or other related parties, reveal negative information, such as a criminal record, involvement in the illegal purchase or sale of drugs, violence, or other potential connections to illicit activity.
- The business, its owner(s), manager(s), or other related parties are, or have been, subject to an enforcement action by the state or local authorities responsible for administering or enforcing marijuana-related laws or regulations.
- A marijuana-related business engages in international or interstate activity, including by receiving cash deposits from locations outside the state in which the business operates, making or receiving frequent or large interstate transfers, or otherwise transacting with persons or entities located in different states or countries.
- The owner(s) or manager(s) of a marijuana-related business reside outside the state in which the business is located.
- A marijuana-related business is located on federal property or the marijuana sold by the business was grown on federal property.
- A marijuana-related business's proximity to a school is not compliant with state law.
- A marijuana-related business purporting to be a "non-profit" is engaged in commercial activity inconsistent with that classification, or is making excessive payments to its manager(s) or employee(s).

Appendix B

BSA/AML Record Retention Requirements

The original, microfilm, electronic, copy, or reproduction of the following documents must be retained for five (5) years:

- All extensions of credit in excess of $10,000 (non-real estate)
- All international transactions in excess of $10,000 (non-real estate)
- Signature cards
- Account Statements
- All checks in excess of $100
- Records to reconstruct demand deposit accounts
- Certificates of Deposit and records of the account holders/purchasers
- Purchase of a monetary instruments of at least $3,000
- Taxpayer Identification number (TIN), separate from backup withholding requirements

For extensions of credit in excess of $10,000 not secured by real estate, the records must include:

- The borrower's name and address
- The credit amount
- The purpose of credit
- The date of credit

For deposit accounts, the records must include:

- The depositor's TIN
- A list of all persons unable to secure a TIN (accounts between 1978-2003)
- Signature cards
- All checks in excess of $100 that are drawn on or issued and payable by the Bank

For Certificates of Deposit, the records must include:

- Customer name and address
- A description of the Certificate of Deposit
- The date of deposit(s)
- A list of all persons unable to secure a TIN (accounts between 1978-2003)

For Funds Transfers or direct deposits, the records must include all deposit slips or credit tickets for transactions in excess of $100.

Documentation of foreign shell bank accounts, the records must be kept for five years after the account relationship is terminated.

Appendix C
ACRONYMS

ACH	Automated Clearing House
AML	Anti-money laundering
APO	Army Post Office
ATM	Automated teller machine
APT	Asset Protection Trust
BCBS	Basel Committee on Banking Supervision
BHC	Bank holding company
BIS	Bank of international settlements
BSA	Bank Secrecy Act
CBQS	Currency and banking query system
CBRS	Currency and banking retrieval system
CDD	Customer due diligence
CFR	Code of Federal Regulations
CHIPS	Clearing House Interbank Payments System
CIF	Customer information file
CIP	Customer Identification Program
CMIR	Report of International Transportation of Currency or Monetary instruments
CTR	Currency Transaction Report
DCN	Document control number
E-cash	Electronic cash
EFT	Electronic Fund Transfer
EIC	Examiner In Charge
EIN	Employer Identification Number
ERISA	Employee Retirement Income Security Act of 1974
FAQ	Frequently asked question
FATF	Financial Action Task Force on Money Laundering
FBAR	Report of Foreign Bank and Financial Accounts
FBI	Federal Bureau of Investigation
FBO	Foreign banking organization
FDI Act	Federal Deposit Insurance Act
FIL	Financial Institutions Letters
FinCEN	Financial Crimes Enforcement Network
FLO	Fleet Post Office
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Intensity Financial Crime Area
IAIS	International Association of Insurance Supervisors
IBC	International Business Corporation
IMF	International Monetary Fund
INCSR	International Narcotics Control Strategy Report
IOLTA	Interest on Lawyer's Trust Accounts
IOSCO	Internal Organization of Securities Commissions
IP	Internet protocol
IRA	Individual Retirement Account
IRS	Internal Revenue Service
ISO	Independent sales organization

ITIN	Individual taxpayer identification number
IVTS	Informal value transfer systems
KYC	Know Your Customer
LCU	Letters to Credit Union
MIS	Management information systems
MLSA	Money Laundering Suppression Act of 1994
NASD	National Association of Securities Dealers
NASDAQ	National Association of Securities Dealers Automated Quotation Systems
NBFI	Non-bank financial institutions
NCCT	Non-cooperative Countries and Territories
NCUA	National Credit Union Administration
NDIP	Non-deposit investment products
NGO	Non-governmental organization
NRA	Nonresident alien
NSF	Non-sufficient funds
NSL	National Security Letter
NYCH	New York Clearing House Association, LLC
OCC	Office of the Comptroller of Currency
OFAC	Office of Foreign Assets Control
OFC	Offshore financial center
OTS	Officer of Thrift Supervision
PEP	Politically exposed person
PIC	Private Investment Company
POS	Point-of-sale
PTA	Payable through account
PUPID	Pay upon proper identification
RA	Regulatory alerts
ROE	Report of Examination
SAR	Suspicious Activity Report
SDN	Specially Designated Nationals or Blocked Persons
SEC	US Securities and Exchange Commission
SSN	Social security number
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TDF	Treasury Department Form
TIN	Taxpayer identification number
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
USC	United States Code