

Customer Identification Policy (BSA)

Approved

November 9, 2006

CUSTOMER IDENTIFICATION POLICY

Policy Statement

As part of Bank's overall compliance with Bank Secrecy Act, it is the policy of Community State Bank to have a clear and concise understanding of all bank customer practices in order to avoid criminal exposure to the bank by any customer who would use the bank's resources for illicit purposes. The objective of this policy is to attempt to ensure the immediate detection and identification of customers and any suspicious activity at the institution.

The bank recognizes that appearances can be deceiving. Potential customers of a financial institution may appear to be legitimate, but in reality could be conducting illicit activities through the financial institution.

It is the policy of Community State Bank to identify bank customers as prescribed by 12 CFR 21 Part 326 and maintain maximum compliance with the US PATRIOT Act. This is done through:

1. Verifying the identity of any person seeking to open an account,
2. Maintaining records of the information used to verify the persons identity, including name, address, type of photo I.D. presented, and other identifying information.
3. Determining whether the person appears on any government lists. Currently, there are no government lists but when there are lists available we will utilize them to identify suspicious individuals or businesses.
4. Procedures for checking our new accounts as well as our entire database for persons we should not be conducting business with are in place with both the Office of Foreign Asset Control (OFAC) and Financial Crimes Enforcement Network (FINCEN).

These directives require the Bank to implement and maintain identification, documentation, verification, and record keeping procedures to ensure:

1. Compliance with state and federal regulations;
2. Adherence to safe and sound banking practices;
3. Decrease the risk that the Bank will become a victim of illegal activities undertaken by a customer;
4. Protect the reputation and strategic position of the Bank with its customers.

Procedures for identifying customers are set out below and will include:

Considerations for maintaining compliance will include but are not limited to the following:

1. Verification procedures will be risk-based
2. Acceptable forms of identification will be outlined below
3. Physical address, if different from mailing address, will be documented
4. Business accounts may be opened if Tax ID number has been applied for but not yet received. In such an instance, a copy of the application must be obtained before the account is opened, or a signatory is added. If the number is not received after 60 days, the account will be closed. The CIP Compliance Officer will assure compliance.
5. Identifying information will be verified within 30 days if at all possible depending on:
 - a. What type of account has been opened,
 - b. Whether all parties are present at opening,
 - c. Type of identification presented and documentation of this photo identification will be maintained for our files.
 - d. If all pertinent information is not obtained within 60 days the account will be closed.

Enforcement

The Board of Directors has approved this policy, and periodically reviews it to make any updates.

Designation of Dawn Snyder as the CIP Compliance Officer and a Bank Secrecy Act Committee to monitor the CIP Policy. The committee consists of the following individuals:

Craig R. Greenland, Customer Service Sales Manager
Sue Briggs, Operations Assistant and BSA Coordinator
Deborah F. McCloskey, Internal Audit and Compliance Officer

Deborah F. McCloskey has been appointed by the Board of Directors as the Internal Audit and Compliance Officer. She will work closely with Dawn Snyder as the CIP Compliance Officer to ensure all aspects of the Customer Identification Policy are in compliance.

Definitions

The term "Account" will include deposit accounts, transaction or asset accounts, and credit accounts

or other extensions of credit. (LIMITED to ongoing transactions and services)

The term “Customer” will include individuals, corporations, partnerships, trusts, and any signatory on an account.

Procedures for Verification of Identity

An integral part of banks Customer Identification Policy is a good knowledge of the transactions carried out by the customers of the bank. Internal systems shall be developed to assist in determining inconsistent activity on behalf of the customer. A Suspicious Activity Report (SAR) will be filed when conduct or transactions appear to be suspicious in nature.

As a general rule, the bank shall not establish a business relationship until the identity of the potential customer is satisfactorily established. It is understood that a community bank such as Community State Bank of Orbisonia has a strong knowledge of the community and the customers it serves; therefore, limited exceptions may be made only when authorized and signed by a senior officer. In all other instances, the following guidelines will be observed.

1. At a minimum, the following information will be collected prior to opening or adding a signatory to any type of account:
 - a. Name
 - b. For individuals, date of birth
 - c. Address
 - (i) For individuals - residence or business street address
 - (ii) Individual who does not have a residential or business street address - an Army Post Office or Fleet Post Office box number, or the residential or business street address of next of kin or another contact individual.
 - (ii) Entity - For persons other than individuals, such as corporations, partnerships, and trusts, principal place of business and, if different, mailing address;
 - d. Identification Number
 - (i) For U.S. persons, a U.S. taxpayer identification number (e.g., social security number, individual taxpayer identification number, or employer identification number);
 - or
 - (ii) For non-U.S. persons, one or more of the following: a U.S. taxpayer identification number; passport number and country of issuance; alien identification card number; or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

Verification procedures will be risk-based. If an existing customer seeks to open a new account, identification was previously verified, and the bank has a reasonable belief that it knows the true

identity of the customer, verification of identification need not be obtained again.

1. Verification through documents: It is the responsibility of Bank personnel to verify a customer's identity via the following documents:
 - a. Individuals - Unexpired government-issued identification, such as a driver's license, passport, etc., that provides nationality or residence and bearing a photograph or similar safeguard.
 - b. Corporations, Partnerships, Trusts and Persons Other Than Individuals - Documents showing the existence of the entity, such as registered articles of incorporation, a government-issued business license, partnership agreement, or trust instrument.
2. Non-documentary verification: It is the responsibility of Bank personnel to properly identify a customer in the event non-documentary methods described above are unavailable in situations where:
 - a. An individual is unable to present an current unexpired government-issued identification document that bears a photograph or similar safeguard.
 - b. The bank personnel are not familiar with the documents presented.
 - c. The account is opened without obtaining documents.
 - d. The account is not opened in a face-to-face transaction; and
 - e. The type of account increases the risk that the bank will not be able to verify the true identity of the customer through documents

Bank personnel are to use one or more of the following alternate methods of identity verification in such instances described above:

1. Directly contacting a customer by telephone or in person;
2. Sending a thank you card or letter;
3. Verifying customer identification with credit reporting agencies and/or a public data base;
4. Physically visiting the customer;
5. Reviewing government lists;
6. Independently verifying documentary information through credit bureaus, public databases or other sources
7. Reviewing a financial statement for credit-related account requests;
8. Obtaining account statements from a previous bank;
9. Checking references with other financial institutions;
10. Obtaining a recent tax return or current financial statement;
11. In the case of the elderly or handicapped individual who cannot produce photo I.D. (never obtained a drivers license, etc.) we will accept the last three months of a current utility bill in their name with current address as an acceptable I.D; and

12. Analyzing whether there is a logical consistency between identifying information provided, such as the customer's name, street address, ZIP code, telephone number, date of birth, and social security or tax identification number.

PERSONAL ACCOUNTS

Identification:

It is the policy of the Bank to properly identify customers with one of the means outlined above.

The customer's residence or place of business:

If it is not in the area served by the bank or branch, ask why the customer is opening an account at that location.

The source of funds used to open the account:

If an unusually large amount of cash is used to open the account, every effort will be made to ascertain the source of the cash.

Service bureau reports.

We reserve the right to pull a service bureau report on any customer opening demand deposit account

Follow-up with a "Thank You" card to the customer's residence or place of employment thanking the customer for opening the account. This will serve as a re-verification of proper address. If the "Thank You" card comes back to the bank undeliverable, by the U.S. Post Office, we will re-verify the address information within the sixty-day time frame from the date of account opening.

A customer may be a referral from a bank employee or one of the bank's accepted customers. In this instance, a referral alone is not itself sufficient to identify the customer.

BUSINESS ACCOUNTS

For corporations, partnerships, trusts and persons other than individuals: documents showing the existence of the entity, such as registered articles of incorporation, a government-issued business license, partnership agreement, or trust instrument.

Check the name of a commercial enterprise with a reporting agency and check prior bank references.

Send a business "Thank You" card to the customer's business address thanking the customer for opening the account. This will serve to verify the address a second time.

When circumstances allow, perform a visual check of the business to verify the actual existence of the business.

Consider the source of funds used to open the account. Question any large cash deposits as to their origin.

Lack of Verification

Depending upon the type of account requested, limited transactions may be permitted in some instances while the identity of the customer is being verified. For example, a personal checking account, opened with funds from a Social Security check, for an individual's personal use, could be allowed to begin using the account immediately, while identity is being verified. However, an account opened by a business with several signatories opened with a variety of funds and a pending tax ID number could be denied access until identification procedures have been completed, and funds have been collected. Risk will determine final policy decisions when there is a lack of ID verification.

In the case of Indirect Lending aka: Dealer Loans, identification and signatures will be requested at the time of application.

When the bank cannot form a reasonable belief that it knows the true identity of a customer, an account will not be opened and a SAR referral form will be forwarded to the BSA Officer.

Procedures for Comparing With Government Lists

It is Bank policy during the customer identify verification process that Bank personnel determine whether a customer (deposit account, loan account, wire transfer, etc.) appears on any list of known or suspected terrorists or terrorist organizations provided to the Bank by any federal government agency. Refer to the Bank's Office of Foreign Asset Control (OFAC) Policy for a detailed description of detection procedures.

If at any time in the process a name matches any suspicious or criminal activity persons list, all procedures will be stopped and the senior compliance officer will be notified. Further investigating will be done before the account opening process resumes. If at any time a legitimate hit is confirmed on any list, the proper Regulatory Agency will be notified immediately. Documentation will be maintained to show that the above process is strictly adhered to.

Recordkeeping

The Bank will maintain a record of the identifying information provided by the customer. When a document is used to verify the identity, documentation of that document including any identifying information it contains, will be maintained. At a minimum, name, address, and other identifying information will be maintained. Documentation of any additional methods of identification will also be maintained. The resolution of any discrepancy in the identifying information obtained will be kept as well. All of these records will be kept for a period of 5 years after the date the account is closed. Under no circumstances will any collection or retention of identifying information be used to make credit decisions on any prohibited basis under the Equal Credit Opportunity Act.

Staff Training

All Bank personnel will receive appropriate training on the Bank's Customer Identification Policy. If at any time an employee has difficulty with a customer or is uncertain about the proper method of handling a situation or transaction, he or she should refer the issue with their immediate supervisor or contact the BSA Officer for further clarification.

Independent Audit Function

Bank will support a process to monitor internal compliance with the above-mentioned policies. This process will include periodic reviews to ensure compliance with laws, regulations, and rulings. In addition, reviews of reporting and control systems will be performed. Written reviews of the above mentioned policies will be completed annually and kept on file for a period of at least 5 years.