

The USA Patriot Act

And Customer Identification Requirements

Prepared By: James Michael Kemp

© Copyright 2005 – All Rights Reserved

A. INTRODUCTION

On October 26, 2001, President Bush signed a new law with a “short title” listed as the “*Uniting and Strengthening America Act by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*” (or just simply the “*USA Patriot Act*”). This law creates or modifies many federal standards under a stated purpose of combating terrorism. Specifically, this law adds or modifies many definitions of criminal conduct, establishes when electronic and technology related communications monitoring may occur, and implements anti-money laundering procedures and safeguards.

You may ask, what does fighting terrorism and the USA Patriot Act have to do with real estate closings? Well, the USA Patriot Act has one specific provision, Section 326, that influences the duties placed upon mortgage lenders, brokers and real estate closing professionals. Specifically, the law requires financial institutions, such as banks, to implement what is known as a Customer Identification Program (“CIP”). Many of you who either attend real estate closings or act as an agent on behalf of a mortgage lender may be somewhat familiar with these “requirements.” This summary will attempt to set forth the specific CIP duties that are placed upon closing agents and their “clients”.

Section 326 of the USA Patriot Act and the CIP implementing regulations found at 31 CFR 103.121, et seq., apply to banks, credit unions, and a broad range of other financial entities such as securities dealers, insurance companies, and check-cashers. These “financial institutions” include real estate closing or settlement agents, and loan or finance companies, See 31 USC 5312(a)(2), as well as any person or entity acting as their agent (i.e. through the delegation of authority, such as when a mortgage broker sells a loan to a mortgage lender).

Financial institutions are required to implement a risk-based CIP that includes a few minimum requirements. The CIP must be in writing and implemented as an integral part of the Bank Secrecy Act (“BSA”) and Anti-Money Laundering (“AML”) programs within the financial institution. Second, the CIP will apply to all customer “accounts”, but not infrequent or occasional interactions such as check cashing or the sale of money orders. 31 CFR 103.121(a)(1). Third, the CIP will be triggered anytime an individual or entity “customer” opens a new account with the financial institution. Existing customers who open a “new” account probably will not trigger the CIP provisions if the financial institution can form a reasonable belief that it knows the true identity of the customer. 31 CFR 103.121(a)(3). Fourth, financial institutions will not be required to verify the identity of account signatories.

There are four “minimum” requirements of a financial institutions’ CIP:

1. Create identity verification procedures
2. Properly document the identity verification
3. Provide notice to the customer
4. Compare verified identities with government lists

B. IDENTITY VERIFICATION PROCEDURES

A financial institution’s CIP entails more than merely making a copy of a customer’s driver’s license, and we will begin review of this process with a description of “identity verification”. First, the customer must provide identifying information. Again, the financial institution must be able to form a “reasonable belief” that it knows the true identity of the customer. 31 CFR 103.121(b)(2). What is reasonable will vary based on many factors, such as the types of accounts offered, the method of opening an account (face-to-face or electronically), the type of information available at the time of the encounter, and the institution’s size, location or customer base.

A CIP must outline the identifying information that new customers must be required to provide prior to establishing the new account, and at a minimum, should include:

For Individuals:

- The full name
- Date of birth
- Residential or business street address
- Identification number

For Businesses:

- Full entity name
- Principal place of business, local office, or physical location
- Identification number

“Identification number” generally means the IRS “Taxpayer Identification Number” associated with the customer, such as a social security number for individuals, or an employee identification number (“EIN”) for most entities. See 31 CFR 103.121(b)(2)(I)(A)

Once the financial institution obtains customers identifying information, the next logical step must be to verify the information within a reasonable amount of time after the account is opened. Generally, verification will occur by the use of documentary evidence, such as driver’s licenses and passports for individuals. The apparent authenticity of that document should be considered, as well as any evidence of fraud or other indications that the document is not authentic such as document alterations or impersonations.

Under 31 CFR 103.121(b)(2)(iii), a financial institution's CIP must describe:

- When the financial institution should not open the account
- The terms under which the customer may use an account while the bank attempts to verify the identity of the customer
- When the bank should close the account when it has failed to verify the customer's identity
- When the financial institution should file a "Suspicion Activity Report"

There are no absolute set of policies or procedures set forth under this law and implementing regulations, and a financial institution may undertake "non-documentary" methods of verification such as contacting the customer outside of the institution, checking references at other institutions or third party sources, or using software or other technology related solutions, as needed.

C. IDENTITY VERIFICATION DOCUMENTATION

Otherwise known as the "record-keeping requirement", a financial institution must keep a minimum of identifying information (name, date of birth, address, and TIN) for five years after the account is closed. All other information obtained must be retained for five years after the record is created. This other information includes:

- A description of any document used to verify the customer identity, noting the type of document, the document identification number, the place of issuance, the date of issuance, and the document expiration date.
- A description of the methods and results of non-documentary measures used to verify identity, if any.
- A description of any substantive discrepancy between the information provided by the customer and that found in identifying methods, with notations as to how the discrepancy was resolved.

31 CFR 103.121(b)(3). Section 326 and the implementing regulations do not require financial institutions to keep copies of documents used to verify identity, such as the drivers license or passport of the customer.

D. NOTICE TO CONSUMERS

All CIP's must include procedures for providing customers with adequate notice that the financial institution is requesting information from them in order to verify their identity. This notice may be given to the customer individually, or in a manner reasonably designated to ensure that the customer is likely to view it (i.e. a sign in the lobby of the financial institution). In 31 CFR 103.121(b)(5), sample language is provided for financial institutions, as follows:

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.

E. COMPARE VERIFIED IDENTITIES WITH GOVERNMENT LISTS

The last minimum requirement for the CIP program is to include procedures for determining whether a customer appears on any federal government list of known or suspected terrorist organizations. It is anticipated that most federal government agencies will utilize the Department of Treasury as the single source of information relating to the creation, compilation, and distribution of a "Section 326" list of suspected individuals for use by the financial institutions. Of course, this is viewed by many as an extremely burdensome requirement of the CIP, and most large financial institutions implement software based solutions to this required task.