Practical USA PATRIOT Act Principles for Banks and Financial Institutions

Learn how the strength of your compliance program determines the strength of your business strategies.

July 2007
**Introduction**

Following the terrorist attacks in September of 2001, Congress passed the USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act). The PATRIOT Act was signed into law in October 2001; its main purpose is to deter and punish terrorist acts in the United States and around the world and to enhance law enforcement investigatory tools.1

Title III of the PATRIOT Act largely impacts financial institutions and addresses terrorist financing and money laundering by expanding existing anti-money laundering laws, primarily the Bank Secrecy Act (BSA). It also more broadly defines “financial institution” so that the scope of money laundering regulations now applies not only to traditional financial institutions (banks, thrifts, savings and loans) but to non-banking financial institutions as well. The new provisions detail required elements in antimoney laundering (AML) efforts and due diligence standards. Financial institutions are now expected to conduct a thorough risk analysis and develop policies and procedures that effectively address the risks identified.

The PATRIOT Act requirements for financial institutions were built on existing standards published by global organizations and associations, and largely adopted as best practice standards. Therefore, the practices mandated by the PATRIOT Act were not necessarily new. However, for organizations that were not formerly subject to BSA requirements, particularly the non-banking financial institutions, the application of AML standards to these industries is undeniably new.

By expanding the definition of financial institution, the PATRIOT Act mandated that AML programs include a sweeping array of businesses. Intricate and demanding, the PATRIOT Act now requires institutions to know their customers like never before. Institutions are expected to conduct due diligence efforts (and enhanced due diligence when necessary) to gain a “reasonable belief” regarding the true identity of each customer. Financial institutions are also required to examine the risks inherent in correspondent accounts and private banking, and address those risks accordingly. The PATRIOT Act encourages communication about suspected terrorists or money launderers by establishing criteria to allow institutions to share their customers’ information with each other, as well as with agency officials.

While the PATRIOT Act is an extensive piece of legislation that affects a large variety of organizations, there are six sections within Title III that are most pertinent to financial institutions: 311, 312, 314 (a), 314(b), 326, and 352. Within these sections, lawmakers laid out instructions about what they expect in terms of due diligence to prevent anti-money laundering and terrorist financing. Some of the instructions on how to implement these regulations are easy to understand. Others are ambiguous and difficult to follow, requiring interpretation and different applications to various situations based upon risk. The following information is provided as a tool to assist you with the intricacies of the PATRIOT Act.

In evaluating requirements set forth in various sections of the PATRIOT Act, you may determine that some sections do not pertain to your business. Trade organizations are often good sources of information about how regulations apply to specific industries. To obtain clarification or further information on regulatory requirements, consult legal counsel or your regulator.

**Why is this white paper important?**

Since it has been several years since their initial implementation, one might expect key concepts of BSA and OFAC (Office of Foreign Assets Control) compliance to be well understood and routinely followed. However, even recently, financial institutions all over the country have failed to comply with these regulations and have been subjected to penalties.
This indicates that a serious lack of preparedness for general compliance remains. The lack of preparedness seems to result largely from:

- Failure to conduct an internal risk analysis
- Inadequate or absent audit components within compliance programs, i.e., a program that is not commensurate with risk
- Failure to designate a compliance officer or manager
- Lack of adequate compliance training

This document is not intended to replace necessary compliance training; rather it is designed to supplement it. In addition, this white paper is not intended to serve as legal advice. Because it summarizes information from various authorities, sources and expert material, this paper serves as a valuable aid in the development of a comprehensive compliance program, including the creation of policies, procedures and controls.

**Organization of white paper**

This paper begins with the relationship of BSA legislation to the PATRIOT Act, discusses AML compliance programs and digs into specific PATRIOT Act sections.

**Note:** As indicated previously, the PATRIOT Act expanded upon the BSA. In this white paper, references to BSA requirements infer parallel PATRIOT Act requirements.

**Bank Secrecy Act: Predecessor to the PATRIOT Act**

Under the BSA, the Secretary of the Treasury is authorized to require financial institutions to establish and maintain AML programs. Because the PATRIOT Act expanded the definition of financial institutions, requirements for AML programs now exist for non-traditional financial institutions, including (but not limited to) casinos, brokers/dealers in securities, insurance companies, futures commission merchants, travel agencies, vehicle dealers and certain jewelry/precious metals dealers, as well as for organizations traditionally seen as financial institutions such as banks, trust companies, loan companies, credit unions and thrifts.

“The BSA was designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions.” As a means to achieve this identification of funds, the BSA requires solid recordkeeping and reporting. These reports and records create an audit trail, which can aid law enforcement in efforts to investigate money laundering crimes. Financial institutions should follow BSA guidelines designed to help reduce the chances that the institution will be a conduit for funds derived from criminal activity.

Compliance programs should provide guidelines for the supervision and training of employees who work with reportable transactions. Employee roles should be defined in a way that segregates the duties of employees who generate and file compliance-related reports from those who make or impact decisions to give customer exemptions. This administrative structure prevents any employee from having complete control and establishes a system where the work of one employee becomes a check on the work of another.

The BSA also requires that regulatory agencies consider the effectiveness of an insured depository institution’s AML program when reviewing any proposed merger. Thus, the success of your compliance program can be a critical component to the strategic plan of your institution.
Risk-based component
An effective BSA/AML compliance program establishes internal controls that are developed in response to an organization’s risk assessment. Therefore, it is critical for an institution to first evaluate its unique risk by considering factors such as customers, their geographic locations and products and services offered to those customers. By conducting a thorough risk analysis, senior management will be able to identify significant vulnerabilities and determine both the likelihood of a money laundering event occurring and the severity of the consequences. A quality compliance program will be tailored to manage those risks according to the risk tolerance of the institution.

Money laundering and other criminal misuses of financial institutions are not new phenomenon. Previously documented cases help define which situations present higher risk of misuse. History has shown that higher risk generally exists in the following types of relationships:
- Private banking and asset management
- Foreign corporations, particularly those licensed as offshore corporations or those privately held and therefore not subject to securities regulatory authorities
- Correspondent accounts particularly with foreign institutions
- Senior foreign political figures

The first step of the risk assessment process is to identify the specific products, services, customers, entities and geographic locations unique to the bank. The second step of the risk assessment process entails a more detailed analysis of the data obtained during the identification stage in order to more accurately assess BSA/AML risk.

When evaluating risk factors, it is important to remember that the amount of risk will vary according to the specific characteristics of each situation. For example, not every transaction in a given location will be of equal risk, and not every transaction by a specific customer will be of equal risk. Scrutinize the entire relationship, combining all factors in order to conduct an effective risk assessment.

Customers
Certain customers pose higher levels of risk. Certain steps are crucial to adequately assess customer risk: establishing the true identity of customers; determining the sources of their funds or wealth; and creating an accurate portrayal of what the relationship should look like. By knowing what is expected, financial institutions are in a position to identify irregular activity and to investigate to determine whether it warrants a Suspicious Activity Report (SAR). It is important that companies refrain from treating all customers in any specific category equally; companies should evaluate all customer-related factors in determining an overall risk level.

Within any category of business, there are account holders that pose increased levels of risk of money laundering. In its “Expanded Examination Procedures,” the BSA/AML Examination Manual suggests businesses that may warrant varying levels enhanced due diligence based upon risk. The following are listed as customers that may require enhanced due diligence:
- Foreign financial institutions, including banks and foreign money services providers (e.g., casas de cambio, currency exchanges, and money transmitters)
- Non-bank financial institutions (e.g., money services businesses; casinos and card clubs; brokers/dealers in securities; and dealers in precious metals, stones or jewels)
- Senior foreign political figures and their immediate family members and close associates, collectively known as politically exposed persons (PEPs)
• Nonresident alien (NRA) and accounts of foreign individuals
• Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies and Private Investment Companies (PICs) and international business corporations (IBCs)) located in high-risk geographic locations
• Deposit brokers, particularly foreign deposit brokers
• Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators and parking garages)
• Non-governmental organizations and charities (foreign and domestic)
• Professional service providers (e.g., attorneys, accountants, doctors or real estate brokers)

In many industries, these concepts are part of a Know Your Customer (KYC) program (also known as CDD or Customer Due Diligence) within the overall compliance program. It makes good sense for businesses to understand their customers, not only for the risks they bring but for the opportunities they present.

**Geographic locations**

Conducting business in certain jurisdictions can be risky; therefore, it is essential to understand the nature, likelihood and severity of risks posed when your business involves other geographic regions, including customers located in or transactions implicating such regions. Many government agencies and international organizations maintain lists of geographic areas considered to present high risk. Organizations are encouraged to evaluate these lists and consider the information they provide when establishing risk-based policies.

These lists can include countries or areas designated as high risk:

- **OFAC**  
  www.treas.gov/offices/enforcement/ofac/sanctions/
- **Patterns of Global Terrorism**  
  www.state.gov/s/ct/rls/c14812.htm
- **Primary Money Laundering Concern under §311 of the PATRIOT Act**  
  www.fincen.gov/reg_section311.html
- **FATF (Financial Action Task Force)**  
  www1.oecd.org/fatf/NCCT_en.htm#List
- **U.S. Department of State International Narcotics Control Strategy Report**  
  www.state.gov/g/inl/rlls/nrcrpt/2005/vol2/html/42388.htm
- **Offshore Financial Centers (OFCs)**  
- **High Intensity Drug Trafficking Areas (HIDTA)**  
  www.whitehousedrugpolicy.gov
- **High Intensity Financial Crime Areas (HIFCA)**  
  www.irs.gov/compliance/enforcement/article/0,,id=107510,00.html

In addition, an organization’s previous experiences with a specific jurisdiction might indicate an increased level of risk. Similarly, current allegations of corruption might be considered when assessing geographic risk. Financial intelligence units (FIUs) may be able to provide additional risk information for a particular area or jurisdiction. The Egmont Group publishes a list of FIUs at: www.egmontgroup.org/list_of_fius.pdf.
**Products and services**
As a general rule, products and services that involve large volumes of currency, those that offer some degree of anonymity and those that involve international transactions are considered to be of high risk. A few examples of high-risk products and services follow:

- Private banking, asset management and trust accounts
- Letters of credit
- Internet banking, ACH, ATMs and other types of electronic banking
- Cashier’s checks, travelers checks and official bank checks
- Credit card lending, lending activity when secured by cash or securities
- Safe deposit boxes
- Foreign correspondent accounts, payable through accounts

Factors alone or in combination may cause an account to be deemed high risk. It is advised that companies scrutinize the entire situation, and combine all factors in order to conduct an effective risk assessment.

**Note:** Using templates for your policies and procedures is no longer recommended since your internal controls must reflect the risks unique to your organization.

**Frequency of risk analysis**
The management team of your institution should update the risk assessment regularly to determine whether there are changes to your organizational risk profile. Businesses typically change over time, and those changes can expose an institution to differing levels of risk. In fact, the most effective risk analyses will be those that are ongoing rather than a one-time exercise. The FFIEC BSA/AML Examination manual recommends that banks reassess their BSA/AML risks at least every 12 to 18 months.5

**Section 352: AML compliance programs**
Section 352 of the PATRIOT Act calls for the development of AML compliance programs for certain financial institutions as defined in the BSA. As discussed in our Introduction, the PATRIOT Act expanded the definition of the term financial institution. As a result, more types of businesses are being required to develop AML programs. For example, in November of 2005, FinCEN published a final rule6 requiring insurance companies to establish anti-money laundering programs.

Section 352 sets forth the expectation that an institution’s AML program will be commensurate with its BSA/AML risks. Thus, a risk analysis is critical. Furthermore, §352 specifies minimum requirements for an AML program. The ultimate goal of an institution’s AML program should be to safeguard its operations from the risks of money laundering or terrorist financing.

Financial institutions subject to §352 should establish a written AML program that includes, “at a minimum:

- the development of internal policies, procedures and controls;
- the designation of a compliance officer;
- an ongoing employee training program; and
- an independent audit function to test programs.”7

---

6 LexisNexis

Practical USA PATRIOT Act Principles for Banks and Financial Institutions

6
Internal controls
Internal controls are written policies and procedures designed to achieve compliance with the BSA and to limit the exposure to AML risk. The program should be approved by the board of directors, which is ultimately responsible for ensuring that the institution maintains an effective AML program.

A risk analysis is a prerequisite to the establishment of an adequate AML program because it identifies those areas of the institution most vulnerable to use by money launderers or other criminals. The nature and complexity of the controls used at any given organization will depend on the risks identified. There are literally thousands of controls, but a few examples commonly included in AML programs are:

- Know Your Customer (KYC)
- Monitoring systems for timely detection of irregular activity
- Identification of activities that warrant reporting, such as Currency Transaction Reports (CTR) or Suspicious Activity Reports (SAR)
- Investigation
- Segregation of duties and systems of dual controls so that employees who fill out forms are not also responsible for filing them with governmental agencies

Designated compliance officer
A competent compliance officer should have both the authority and resources to ensure overall compliance with the AML program. Ideally, the compliance officer would report directly to the board of directors, but at a minimum, there should be a direct line of communication between the compliance officer and the senior most level of management. For example, the compliance officer should inform the board of directors of changes to the BSA or new developments in its related regulations. The compliance officer should coordinate and monitor day-to-day compliance activities, and be responsible for making sure the organization meets regulatory requirements. It is essential that he or she develop expertise in AML and terrorist financing laws and regulations. It is also critical that he or she understand the financial institution’s products, services, customers and geographies and the risks associated with each. Some organizations formally designate more than one person to manage the duties typically assigned to the compliance officer position.

Employee training
Section 352 requires that employee training be an integral component of an AML compliance program. Because the BSA and its related regulations change, training should be ongoing and incorporate recent developments so that all employees remain current. Training should provide an overview of the BSA and its regulations, plus definitions of money laundering and terrorist financing and descriptions of current criminal schemes. In addition, a presentation of the most vulnerable areas within an institution and
employees’ roles and responsibilities in combating money laundering and terrorist financing should be covered.

The training program is one area where an institution can truly reinforce a compliance culture. Best practices standards dictate customizing training to the roles of the attendees. For example, bank tellers might receive training on CTRs. Loan personnel might learn about recent money laundering typologies involving mortgage loans. Compliance personnel might receive training on investigating irregular account activity and on correctly completing SAR forms.

The board of directors should be made aware of general concepts required in BSA risk management. It is appropriate and expected that the board will delegate BSA duties; however, they should understand their role in oversight and their responsibility in overall compliance.

Institutions should provide training to all new employees, and compliance officers should keep executives informed of breaking developments in BSA regulations. Refresher training should be made available according to a schedule agreed to by senior management. Personnel in key positions, such as those who interface with customers at account opening, those who handle cash transactions, those who process wire transfers and those who work with investments or loans should have more frequent training. Refresher training should also be given when regulations change, or when internal policies or procedures change.

As with all compliance activities, it is critical that you document all training activities and make copies of training materials so that they can be made available for review by examiners.

In order to determine whether your training program is effective, you should test students for content knowledge and audit the activities of personnel. Knowing what to do and choosing to do it are two different things. An examination at the conclusion of a training session will test for comprehension of compliance regulations, but an audit will show whether the knowledge transferred to the work place. If the audit indicates inadequacies in any particular area, make relevant training a top priority.

**Independent audit**

Legislation within the PATRIOT Act presents an opportunity for institutions to continually review their compliance programs and make improvements. This component of an AML program creates a safety net and provides confidence that your program is working as planned. Ensure that there is an ongoing self-monitoring effort, particularly for the reporting requirements of BSA, to either validate the process or catch and correct errors in procedures as quickly as possible. If the program is risk based, auditing procedures should focus on those areas that present greatest vulnerabilities.

Compliance tip

As part of your compliance effort, make training a top priority. Employees in every position should be able to perform their specific responsibilities in relation to the AML program and relate those responsibilities to vulnerabilities. Also, document employee test results and make these available for examiner review.
Companies may use a qualified internal employee to audit or contract with an external auditor. If internal personnel are the auditors, they should have solid AML expertise but should not be involved in the function being tested. A report containing the audit findings should be presented directly to the board of directors and senior management, who will subsequently determine the appropriate course of action.

While the frequency of audit is not specifically defined in any statute, a sound practice is for [institutions] to conduct independent testing generally every 12 to 18 months, commensurate with the BSA/AML risk profile. Failure to test and correct programs accordingly can create a heavy burden well beyond monetary penalties. Violations can and will result in strict regulatory supervision of the institution’s compliance efforts and program. Depending on the seriousness, outside consultants may be required. It is likely that rigid and regular reporting to the institution’s board of directors would be required of the compliance program. Furthermore, the board would be required to respond to all reports, make recommendations and follow up on findings.

As with all risk-based audits, auditors should test the entire program but focus their efforts on the areas of highest risk. Without fail, they should refer to previous audit reports to verify that any corrective actions have been implemented and are effective.

Section 352 checklist
• Create and implement internal written policies, procedures and controls to comply with BSA.
• Designate a compliance officer.
• Establish an ongoing employee training program.
• Implement independent audit functions.

Section 326: Customer Identification Programs
Section 326 of the PATRIOT Act required the U.S. Secretary of the Treasury to develop regulations setting forth minimum standards regarding customer identification for opening new accounts at certain financial institutions. The statute set minimum requirements requiring financial institutions to implement, and customers (after being given adequate notice) to comply with, reasonable procedures for:
A. Verifying the identity of any person seeking to open an account to the extent reasonable and practicable;
B. Maintaining records of the information used to verify a person’s identity, including name, address and other identifying information; and
C. Consulting lists of known or suspected terrorists or terrorist organizations. 
The result was the development of a joint regulation by the federal banking regulatory agencies to implement Section 326. That regulation is now called “the CIP rule” because it requires banks, savings associations, credit unions and certain non-federally regulated banks to have a written Customer Identification Program (“CIP”).

Who must comply?
Due to the expansion of the definition of financial institution, the joint final CIP rule applies to a variety of financial institutions, including nonbank or non-traditional financial institutions. The final rule was published in the Federal Register on May 9, 2003, with the following clarification:

• Section 326 applies to all “financial institutions.” This term is defined very broadly in the BSA to encompass a variety of entities, including commercial banks, agencies and branches of foreign banks in the United States, thrifts, credit unions, private banks, trust companies, investment companies, brokers and dealers in securities, futures commission merchants, insurance companies, travel agents, pawnbrokers, dealers in precious metals, check-cashers, casinos and telegraph companies, among many others.

Possible exempt institutions or accounts
There may be instances when a federal regulator, with approval from the Secretary of the Treasury, exempts a financial institution, by order or regulation, from meeting CIP requirements. Such an exemption could also pertain to a type of account. Should an organization gain an exemption from §326, the organization would still be required to comply with other BSA regulations.

Reliance on another financial institution
Financial institutions frequently use third party service providers as agents to establish relationships with customers. Two examples are car dealers and mortgage brokers, who may act as a bank’s agent in connection with a loan. While it is acceptable for a bank to delegate to its agent the performance of some or all of the bank’s CIP activities where it is reasonable to do so under the circumstances, the bank remains ultimately responsible for that agent’s compliance with the rule. For this reason, the agent’s policies and procedures should be audited periodically to be sure that all minimum requirements are met.

Procedures delegated may include any of the following:
• Providing adequate notice that personally identifying information will be requested
• Collecting identity information and/or verifying the person’s identity
• Determining whether a customer appears on a government terrorist list, and
• Keeping the records for a period of five years after the account is closed.

There is a second situation in which a bank may use an agent to perform the tasks required under the bank’s CIP rule. This occurs through what is called “the reliance provision”, which permits one financial institution, in limited circumstances, to rely on another to perform any of the elements required to be in a bank’s CIP.

This is only allowed if both institutions are regulated by a federal functional regulator and are subject to a general BSA compliance program rule, they share the customer and the bank can show its reliance upon the other financial institution is reasonable under the circumstances. In addition, a contract must be signed annually, and certifications must be provided.

Customer Identification Programs
The CIP minimum standards are intended to enable financial institutions to form a reasonable belief about the true identity of each customer.
Many institutions had existing KYC procedures in place that were comparable to the CIP rule requirements. In order to meet the mandates of the joint final rule, you should:

- Conduct a risk assessment, and make sure your procedures include practical risk-based identification steps that are appropriate to the size and type of your business.
- Review your existing written policies and procedures and amend them to include any missing regulatory requirements.
- Make sure your account opening procedures enable you to form a reasonable belief that you know the true identity of each customer.

CIP structure
Your CIP must:

- Be documented and incorporated into your overall BSA program (if BSA is a requirement for your institution).
- Be formally approved by your board of directors.
- Be tailored to suit the aspects of risk according to your institution’s size, location and type of business.
- Contain policies and procedures to address:
  - Providing notification to customers of the required information collected
  - Collecting particular information on all new customers
  - Taking steps to adequately verify the information provided
  - Checking all new customers against government watchlists (the lists required have yet to be determined at the time of publication of this document)
  - Retaining customer records

Each of these elements is more fully described below.

Accounts subject to Section 326
CIP procedures apply when a new customer opens an account in order to receive services from the financial institution, or when a customer already receives services. The customer may be an individual, a corporation, partnership, a trust, an estate or some other entity recognized as a legal person.) Such services may include:

- Establishment of ongoing business relationship
- Deposits
- Asset management
- Loans, credit accounts and other extensions of credit
- Transactions or asset accounts
- Safe deposit box or safekeeping services
- Custodial accounts
- Trust services

For purposes of §326, a customer does not include a person who does not receive banking services, such as a person whose loan application is denied. It also does not include a person who fails to establish a formal ongoing business relationship, such someone who cashes a check (unless he or she cashes checks frequently) or who purchases a money order.*

* However, an institution should be aware that other laws and regulations concerning customer identity and transaction monitoring may apply to these transactions.
Existing customers
When an existing customer opens a subsequent account, there is an exemption to applying CIP procedures provided that you have a reasonable belief that you know the true identity of that person. This concept applies whether an existing customer opens a secondary account, renews a loan or rolls over a Certificate of Deposit. In these cases, the financial institution need not follow CIP procedures to establish the true identity of the customer as long as the institution has a reasonable belief that it already knows the customer’s true identity. You should be aware that regulators may require the institution to demonstrate that it knows the customer’s true identity. This can be accomplished by providing proof that the information gathered from the customer was substantially the same as that required under the CIP rule. It may also be demonstrated by showing evidence of a long-term and active relationship with the customer, with no signs of risk.

If a spouse becomes a new holder on an existing account, then that spouse is a new customer subject to the CIP rule, and identity information collection and verification would be necessary.

CIP compliance procedures

Notify customers
The CIP must include procedures for providing customers with a notice that the financial institution is requesting identifying information. The notification must be provided in a manner that ensures it is seen or received by customers before identifying information is requested (i.e. lobby poster, notice on the institution’s website, sign on customer service representatives’ desks, printed on the account application, etc.).

The following sample text is provided in the regulation:

Important information about new account opening procedures
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 is that 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.
Collect customer identity information
The CIP final rule specifies that financial institutions must require new customers provide at a minimum, the following information when they open a new account:

- Name
- Physical address (Active military personnel may provide a Fleet or Army PO box)
- Date of birth
- Tax-payer ID number or similar officially-issued identification number

Acceptable documents for identity verification include:

- For U.S. persons, unexpired:
  - Taxpayer identification number (Social Security number (SSN) or employer identification number (EIN))
  - Passport number (including country of issuance)
  - Drivers license
  - State-issued ID card
- For a non-U.S. person, unexpired:
  - Taxpayer identification number
  - Passport number (including 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

A new account may be opened for a customer who has applied for, but has not received, a taxpayer identification number. The CIP must include procedures to confirm that an application was filed prior to account opening and to obtain the number within a reasonable period of time.

Verify new customers’ identities
After collecting the required information from customers, you must take steps to verify the customers’ identities. In most cases, you will use documentary methods. However, you may also choose nondocumentary methods to verify identities.

Documentary methods
Institutions are not required to verify each piece of documentation gathered from customers, but they should verify enough to form a reasonable belief of each and every customer. Your CIP must establish the minimum acceptable documents that are acceptable, as well as the minimum verification steps required. The list of documents suggested above has long been used by banks to establish identity, and many institutions will continue to use these documents. However, other documents may be used, as long as the ultimate goal of knowing your customer’s true identity is met.

One advantage of using the documents from the list above is that your personnel may be able to spot counterfeit or fraudulently obtained documents a bit more easily.

Nondocumentary verification methods
No institution is required to use nondocumentary methods to verify a customer’s identity, but an institution can choose to do so. The CIP policies, procedures and controls must precisely define the situations where nondocumentary methods are appropriate, and must specify efforts required in different situations.
CIP nondocumentary procedures should address the following situations:

- A customer is unable to provide an unexpired government issued photo ID or when the institution is unfamiliar with the document provided.
- A customer does not open the account in person and does not provide identification documents.
- A customer opens an account without physically visiting the institution.
- An institution is otherwise presented with circumstances that increase the risk that the institution will not be able to verify the true identity of the customer through documentation.

Examples of nondocumentary methods that you might employ include:

- Contacting a customer for identifying information by:
  - Visiting the business site to establish its existence
  - Calling the telephone number provided
  - Verifying mail has been delivered or verifying mail has not been returned
- Comparing information provided by the customer to a third-party source or public records information
- Checking references with other financial institutions
- Obtaining reviewed or audited financial statements

Verifying your customer’s identity might include steps such as:

- Checking the SSN provided by your customer against the list of deceased persons SSNs.
- Making sure the SSN number is valid, or that the number pattern fits place of birth, date issued, etc.
- Verify address is real through:
  - Checking the information provided against public records information.
  - Visit the customer, especially if business.
- Call the customer.
- Check references.
- Obtain credit reports.

Special methods for certain customers
An institution will undoubtedly need to verify the identity of an account holder that is not an individual, as in the case of trusts, corporations, partnerships, sole proprietorships, etc. In some cases, the institution may be unable to verify the identity of the entity using standard documentary or nondocumentary methods. In these situations, an institution may need to obtain personal identifying information from an individual with authority or control over the account even though he or she is not the named account holder. Your CIP should specifically state when these alternative methods are acceptable, and what information should be collected. In the case of legal arrangements, such as corporations or

Compliance tip
Leverage information submitted to other departments. For example, you may carry a loan, an annuity or investments for this customer, and in those records you may find additional information to verify identity. However, there are other regulations controlling the appropriate sharing of information. Be sure that your efforts towards identity verification do not conflict with other regulations.
partnerships, you should obtain documents that validate their existence. Such documents may include a business license issued by a government body, articles of incorporation, or a certified document showing incorporation, or a formal agreement indicating partnership. In order to verify a partnership’s identity, institutions should undertake additional verification by obtaining information about the identity of any individual with authority or control over a partnership account.

**Note:** Your compliance policies, procedures and controls must indicate when your institution will allow the use of alternative methods, what processes must be performed as part of those methods, and exactly what results must be obtained to make the alternative methods an acceptable form of identity verification.

**Enhanced due diligence procedures**

Due diligence procedures result in the information required of all customers. Enhanced due diligence procedures supplement standard due diligence and are invoked when more information is necessary due to perceived risk or the need to reach a higher level of confidence associated with the relationship. The CIP should be “reasonably designed” to detect and report instances of money laundering. Enhanced due diligence procedures may include efforts such as:

- Requiring senior management approval for establishing the account
- Requiring senior management approval for certain transactions
- Lowering the threshold or escalating the frequency for monitoring transactions
- Establishing the source of wealth and source of funds
- Frequently and thoroughly reviewing the client profile

**Lack of verification**

An institution’s CIP must include procedures to follow when it is unable to form a reasonable belief that it knows the customer’s true identity. The policies must determine actions to be followed when a new account:

- Will not be opened.
- May be opened pending the identity being verified.
- Will be closed after identity verification methods fail.

CIP policies and procedures should include a description of the circumstances under which an institution should file a SAR (Suspicious Activity Report) for events related to account opening or CIP processes. These procedures should be in accordance with applicable laws and regulations beyond §326.

---

**Compliance tip**

Separate from the obligation to maintain records gathered in determining customers’ true identity, keep a log of steps taken in nonstandard situations. Document the situation and the decisions made, along with the decision-making criteria used. This information will be valuable in the event of an audit, whether internally or externally administered. Use this documentation as an aid in your training program.
Check watchlists
The CIP must include procedures to compare customer names to federal government-issued terrorist watchlists. At the time of publication of this white paper, no single government list has been issued. Authorities continue to indicate that a list is forthcoming. In the interim, financial institutions should compare the names of customers seeking to open an account against various government-issued lists containing the names of known or suspected terrorists or terrorist organizations.

Watchlists to consider for terrorist screening include the following:
• OFAC Specially Designated Nationals and Blocked Persons
• OFAC Non-SDN entities (currently, the PLC list)
• OFAC Sanctions Program and Country Summaries
• Terrorist Exclusion List
• UN Consolidated List
• FBI lists:
  - Seeking Information
  - Most Wanted Terrorists
  - Hijack Suspects

Any similar list specific to jurisdictions presenting risk to the organization. Examples include the European Union Consolidate List, the consolidated list from the Office of the Superintendent of Financial Institutions Canada, Australia’s Department of Foreign Affairs and Trade list, the Hong Kong Monetary Authority list, Monetary Authority of Singapore list, etc.

Retain records
The CIP must include record retention procedures:
• Customer identifying information collected at account opening (name, address, date of birth, tax identification number (TIN) and any other information required by your CIP) are to be retained for a minimum of five years following account closure. In the case of credit cards, the customer identifying information must be retained for five years after the account either closes or becomes dormant.
• A description of the documentation and method used to verify identity must be retained for five years after an account is created. Retaining an actual photocopy of the documents is not necessary (although it is permitted), and in fact may introduce new risks unrelated to BSA. You should, however, retain a detailed description of the documents used, including a narrative of the type of document presented, the person who inspected it, the ID number, place and date of issuance and expiration date.

Compliance tip
Some compliance professionals suggest that institutions retain the four key pieces of identifying information (name, physical address, government ID and date of birth) for the life of the account.
Section 326 checklist

- Review existing AML policies, procedures and controls with regard to assessing institutional risks
- Develop and document CIP policies, procedures and controls for:
  - Notifying customers that identifying information will be collected
  - Checking client data against government watchlists
  - Verifying the identity of new account holders using reasonable and practical assessment methods
  - Employing enhanced due diligence for situations when unable to verify identity, including when to:
    - Open an account (permanently or conditionally)
    - Close an account
    - File a SAR
    - Recording steps taken and decisions made in non-standard situations when trying to verify identity
    - Retaining records of customer identification information
    - Auditing your CIP program
    - Training employees
- Obtain written approval from your board of directors for your CIP

Section 312: Correspondent and private banking accounts

Section 312 of the PATRIOT Act addresses money laundering risks associated with correspondent accounts and private banking relationships by requiring U.S. financial institutions to apply enhanced due diligence measures. The standards for enhanced due diligence generally include determining the true identity of the account owners, conducting enhanced scrutiny of such accounts and reporting suspicious transactions.

Section 312 states that each financial institution that establishes, maintains, administers, or manages a private banking account or a correspondent banking account in the United States for a non-U.S. person (including a foreign individual visiting the United States), or a representative of a non-U.S. person will create AML policies. The AML policies should establish appropriate, specific, and where necessary, enhanced due diligence policies, procedures and controls that are reasonably designed to detect and report known or suspected instances of money laundering through those accounts. For further detail, see the BSA 31 U.S.C. 5318(i).

Private banking accounts

As defined in §312, a private banking account of a foreign individual refers to an account or combination of accounts whose assets total at least $1,000,000. It also refers to those accounts initiated by individuals who have direct beneficial ownership of the account. The accounts..
referred to are typically managed by assigned representatives of the covered institution acting as direct liaisons to the beneficial owners. These representatives are often officers, employees or agents and are typically referred to as private bankers.

Because of the risk associated with private banking, §312 called for enhanced due diligence policies, procedures and controls to guard against money laundering and foreign corruption. These procedures should include the verification of identity of all account holders and beneficial owners, or those who effectively exercise control over the assets. Regulations and guidance issued relative to private banking accounts advise institutions to gather information on business lines involved, source of funds, source of wealth and nature of the anticipated transactions.

Covered financial institutions should check the names of account or beneficial ownership holders against lists of senior foreign political figures (SFPF), their immediate family members and close associates. These individuals are commonly referred to as politically exposed persons (PEP), and are generally considered to be at higher risk for money laundering. When offering private banking services (high risk product) to politically exposed persons (high risk customer), the risks are compounded. For this reason, §312 requires institutions to conduct enhanced scrutiny of private banking accounts if they involve SFPFs. While the regulation specifies $1 million, PEP risks may be present for accounts whose assets fall short of that threshold.

The requirement under §312 applies only to senior foreign political figures (e.g. current or former senior officials in a foreign government, whether working or located in the U.S. or a foreign country); however, both money laundering and terrorist financing cross international borders. Therefore, most global organizations concerned with battling these crimes recommend that institutions apply the same due diligence standards to domestic PEPs as well. If you suspect or determine any violation of law conducted through or involving a private banking account, this information must be reported. Your policies and procedures should include how such violations will be reported.

Correspondent accounts
Correspondent accounts are those relationships between a U.S. bank and foreign bank where accounts are established to provide regular services. The services might include receiving deposits, distributing payments, extension of credit or other financial transactions, but it is intended to apply to regular and ongoing relationships. Section 312 establishes due diligence standards for correspondent accounts if the account is requested by, maintained by or on behalf of a foreign bank operating under:

- An offshore banking license
- A banking license issued by a foreign country that is designated as non-cooperative with international AML principles of an organization like the FATF

Compliance tip
Your regulator may require you to conduct additional scrutiny on specific countries known to be at high risk for money laundering but not designated by FATF, the Treasury, or the State as primary money laundering concerns. Refer to the section entitled Geographic Locations for further information about jurisdictional risk.
• A banking license issued by a foreign country identified by the Secretary of the Treasury as warranting special measures due to money laundering concerns

The required enhanced due diligence policies, procedures and controls for correspondent accounts, at a minimum must ensure that the U.S. financial institution takes reasonable steps:

• To scrutinize the account to identify and report suspicious activity
• To determine the identity of each of the owners of the non-publicly traded foreign bank, along with the nature and extent of the ownership
• To determine whether the foreign bank provides correspondent accounts to other foreign banks, and if so, to apply enhanced due diligence to these nested banking relationships

Section 312 checklist
• Develop and document policies, procedures and controls for:
  • Collecting identity information on foreign nominal and beneficial account holders.
  • Verifying that these entities are not PEPs.
  • Ascertaining actions to be taken if customer identified as a PEP.
  • Reporting suspected violations.
  • Identifying foreign bank licensing and verifying entities are not licensed in a country designated by FATF as non-cooperative.

Section 311: AML for foreign jurisdictions

Section 311 of the PATRIOT Act authorizes the U.S. Department of the Treasury to designate international financial institutions, foreign jurisdictions and specific types of accounts or classes of transactions as being “of primary money laundering concern.” The Treasury is authorized to impose special measures upon these entities.

In general, § 311 grants the Secretary of the Treasury authority to impose one or more of five special measures, ranging from additional record keeping and reporting requirements to prohibitions on certain payablethrough or correspondent accounts. The five measures can be combined to create an option specifically designed to target a given money laundering or terrorist financing concern. Thus, additional due diligence, and sometimes the restriction of available services, is required when dealing with accounts with these designations.

The Secretary of the Treasury is required to consult with the Secretary of State and the Attorney General prior to designating a primary money laundering concern (PMLC). When deciding which of the special measures to impose, the Secretary of the Treasury will consult with federal functional regulators or other interested parties as appropriate.

The five special measures
The first measure allows the Treasury to require U.S. financial institutions to collect and/or report information about transactions with a PMLC, including the identity and address of each participant and originator of any funds transfer, the beneficial owners of the money, amounts involved, a general summary of the transaction or any other relevant data about a transaction.

In the second measure, the Treasury may require domestic financial institutions to conduct enhanced due diligence to determine accurate beneficial ownership of an account opened in the United States by a foreign person involving the PMLC.
Under the third measure, institutions that maintain payable-through accounts in the United States for foreign financial institutions in jurisdictions designated as PMLCs may be required to obtain identification documents from each customer permitted to use the account or whose transactions are routed through the account. An institution may also be required to maintain the same type of identifying information collected from its customers residing in the United States.

As part of the fourth special measure, U.S. institutions who maintain a correspondent account involving a PMLC, as designated under §311, will be required to obtain identity verification data comparable to what they obtain for domestic customers, but for all persons involved with the correspondent account.

These record keeping and reporting orders are effective for a limited time, and may be extended by regulation. Institutions are advised to monitor the status of the order.

Under the fifth special measure, the financial institution may be prohibited from opening or maintaining correspondent or payable through accounts involving a PMLC. Regulations implementing an order may require an institution to take steps to prevent the PMLC from gaining indirect access to the financial institution.

When dealing with any PMLC, an organization should review the Treasury regulations and orders imposed by the Secretary of the Treasury to determine which of the special measures have been imposed, and what information and activities are required under that special measure. Remember that the orders and the resulting requirements may change over time.

**Section 311 checklist**

- Obtain a list of entities and jurisdictions designated by the Treasury as being of primary money laundering concern.
- Determine the required action(s) for each designee under the corresponding order or regulation.
- Train employees on §311-related risks and their roles in mitigating it.
- Develop and document policies and procedures for:
  - Checking customers against watchlists consistently.
  - Taking actions on accounts and transactions when a potential match is identified.
  - Notifying your regulator in the case of a positive match.
  - Following notification requirements in the case of a positive match.

**Compliance tip**

Review an alphabetic or chronological list of actions taken under Section 311 at FinCEN’s “Section 311 – Special Measures” web site http://fincen.gov/reg_section311.html
- Record keeping for:
  - Customer information.
  - Actions taken.

Section 314: Special information sharing

Section 314 of the PATRIOT Act encourages the sharing of information regarding terrorist financing and money laundering between financial institutions and the law enforcement community. It directed the Secretary of the Treasury to adopt regulations encouraging further cooperation among financial institutions, their regulatory authorities and law enforcement authorities, with the specific purpose of sharing information regarding individuals, entities and organizations suspected of engaging in terrorist acts or money laundering activity. Central to these efforts is the Financial Crime Enforcement Network (FinCEN), a network, the purpose of which is to bring together the law enforcement, regulatory and financial communities, thereby facilitating the exchange of information among the network partners.

Section 314 is comprised of two parts or subsections, (a) and (b). Section 314(a) called for regulations to authorize law enforcement, through FinCEN, to investigate suspected money launderers and terrorists by asking financial institutions to identify accounts related to the suspects. Section 314(b) establishes a mechanism for financial institutions to share information about suspected money launderers and terrorists with each other.

FinCEN requires that requests being forwarded to financial institutions represent only the most significant investigations from each of the law enforcement agencies*. All federally regulated financial institutions are required to assist law enforcement in their investigations by participating in the 314(a) process, but by vetting the requests, FinCEN minimizes the burden on financial institutions and maximizes the effectiveness of the information sharing system.

Section 314(a)

FinCEN publishes a list of subjects against which federally regulated financial institutions must search. The list is published on FinCEN’s secure website every two weeks. An institution should search both transactions and account records at its head and any branch offices operating in the United States. The institution must conduct a search to determine if it maintains accounts for, or has in the past maintained accounts for, or has engaged in any transactions with any individual or entity named on the 314(a) list. Generally, institutions should compare the 314(a) list against accounts maintained by named individuals or entities looking back 12 months and transactions looking back 6 months. For more information, go to www.fincen.gov/fi_infoappa.html.

The search performed by the institution:

- Will be a one-time search, unless otherwise indicated in the instructions
- Must be completed within 14 calendar days unless the institution is otherwise advised in the accompanying instructions
- Must include:
  - Deposit accounts
  - Incoming wire transfers—the recipient or beneficiary
  - Outgoing wire transfers—the originator of bank check

* To ensure that this standard is met, FinCEN requires documentation showing the size or impact of the case, the seriousness of the underlying criminal activity, the importance of the case to a major agency program, and any other facts demonstrating its significance. See Financial Crimes Enforcement Network, FinCEN’s 314(a) Fact Sheet, January 2007, <http://www.fincen.gov/314afactsheet.pdf> (Jun. 1, 2007).
- Sales of travelers checks, money orders and cashier’s checks between $3000 and $10,000
- Loans
- Trust accounts
- Securities accounts
- Commodity, futures, options, or other derivatives accounts
- Safe deposit boxes: the renter plus all authorized to access account

• Must search against:
  - Accounts maintained during the preceding 12 months
  - Transactions (not linked to an account) conducted during the preceding 6 months

A match occurs when a financial institution determines that it has located an account or a transaction corresponding to one of the subjects on the §314(a) list. A financial institution should use all of the identifying information provided to determine whether or not there is a “true” match. If the 314(a) list is incorporated into a software application, false positives are possible. A financial institution should contact the requesting law enforcement agency for further guidance if it is unable to ascertain whether it has a true match. For each name presented on the 314(a) list, the corresponding law enforcement agency is indicated.

For each true match identified, the institution is to report match information to FinCEN. The institution should provide the matched name and contact information for a person within the institution should law enforcement need to obtain additional information. Further action is not required unless the institution is contacted by the requesting law enforcement agency.

**Important:** It is not necessary or required for the institution to reject transactions, or close or block an account that obtained a 314(a) match unless advised to do so. In fact, additional actions may not only interfere with investigations, but may actually violate other regulations. For this reason, it is important for institutions to develop procedures that maintain strict confidentiality when disbursing the list to those persons assigned with executing a 314(a) scan.

**Confidentiality and record keeping**
Confidentiality regarding your request for information from federal law enforcement via FinCEN is extremely important. Please note the following guidance regarding search confidentiality and record keeping:

• Institutions are to designate one or more staff members to serve as central point of contact for FinCEN requests. This will help to ensure confidentiality and appropriate care with required steps in searching records and recording information.

• Search requests are confidential and are not to be disclosed to the target of the search. Personnel involved in executing the search must not disclose the FinCEN 314(a) list information or results to anyone other than the primary contact.

• An audit trail should be maintained for a reasonable amount of time. The audit trail should document the records searched and log any notations made. Due to the extreme sensitivity of the names on the list, keeping a copy may not be advisable. While the length of time to retain your audit log is not specified in the regulation, five years is the current best practice standard for retaining records of 314(a) searches. Consult FinCEN, your regulator or legal counsel for further guidance.

If you are asked by anyone other than a law enforcement agency about a specific entity on a 314(a) list, contact your legal counsel immediately. If you are asked by an outside attorney in a discovery request, you should call your legal counsel and the law enforcement agency indicated on the 314(a) request immediately.
Section 314(a) checklist

- Designate a FinCEN contact person in your organization.
- Provide adequate training to designated contact.
- Develop and document policies and procedures for:
  - Verifying current customers, and those active in the last 12 months, against FinCEN list within two weeks of its receipt
  - Verifying all non-account related transactions (such as wire transfers, currency exchange, etc.) within the last six months against FinCEN list within two weeks of its receipt
  - Reporting positive matches to FinCEN
  - Responding to any instructions provided with the list or provided after a positive match is identified
  - Keeping records for a suitable time to establish an effective audit trail

Section 314(b)

Section 314(b) permits financial institutions or associations of financial institutions to share information regarding money laundering or terrorist financing with each other as a matter of courtesy or necessity, as in the case of affiliates. Sharing information is not mandatory; however, if an institution shares information, it must provide notice to the Secretary of the Treasury in advance.

Safe harbor

A safe harbor exists from liability for sharing information about an individual or organization who is a suspected terrorist or money launderer. In order to be afforded the safe harbor provisions of 314(b), both financial institutions must notify FinCEN of their intent prior to information sharing. A notice to share is valid for one year. Instructions on submitting a notification form, whether the initial form or a renewal, can be found at: www.fincen.gov/314b_main.html.

Information sharing between financial institutions is afforded safe harbor if the information involved will be used solely for preventing money laundering or terrorist financing activities.

In order to share information and have safe harbor from civil liability:
- You must file an Intent to Share notice with FinCEN.
- You must take reasonable steps to verify that the financial institution or association with whom you intend to share information has submitted its 314(b) certification notice. FinCEN has indicated that it will intermittently publish a list of financial institutions or associations that have filed notices.
- You must certify that you have policies and procedures that safeguard the privacy of customer information and appropriately limit your use of the information, including to identify or report money laundering or terrorist activities, or to determine whether to maintain an account or engage in a transaction.
- You should identify a contact person at your financial institution.

Confidentiality

Institutions that share information must protect confidentiality of the information contained in this file request. Be certain policies, procedures and controls address this need directly.

Information shared between financial institutions must also be shared with the federal government when the financial institution suspects that an individual, entity or organization is or may be involved in terrorist activity.
Situations involving suspected terrorist activity or ongoing money laundering activities require immediate attention. Reports should be made immediately by calling an appropriate law enforcement authority, or the toll-free Financial Institution Hotline (1.866.556.3974), and, if appropriate, by filing a SAR (suspicious activity report). Nothing in this section limits or otherwise affects the obligation to file SARs or other reporting as required of suspected terrorist activities.

Section 314(b) checklist

- Create policies and procedures for:
  - Notifying FinCEN and refiling yearly
  - Verifying other cooperating institutions have filed with FinCEN
  - Protecting security and confidentiality of customer data
  - Limiting information to the situations involving suspected money laundering or terrorist financing

Additional information

If financial institutions have additional concerns or questions, they should contact their federal functional regulator or FinCEN at the FinCEN regulatory helpline at 800.949.2732 or www.fincen.gov.

What examiners will look for

On June 30, 2005, the Federal Financial Institutions Examination Council (FFIEC), a group of financial regulatory agencies, issued a 330-page manual on unified standards for bank examiners. The Bank Secrecy Act / Anti-Money Laundering Examination Manual is scheduled to be updated annually, and the 2006 revision is available at www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm. The Examination Manual serves to promote consistency in oversight and supervision of financial institutions by both federal and state agencies. Expect your examination to be risk-based; meaning that, while examiners will evaluate the internal control system as a whole, they will focus on those areas perceived as most vulnerable to money laundering or terrorist financing. You can expect examiners to tailor each examination to the risk profile of your institution, including documents requested, areas to be tested, the depth of the testing in those areas and the number of personnel assigned to the audit. Thus, it is likely that not all internal control procedures will be tested equally.

A thorough review of the current examination manual will enhance your understanding of, and ultimate compliance with, the legal and regulatory requirements. Examiners will undoubtedly request your risk analysis early in the process. They will plan procedures and resources accordingly, but may need to use additional core or expanded examination procedures when they arrive on site. They will incorporate transaction testing to assess the adequacy of the compliance with regulations, measure the effectiveness of the policies and procedures and evaluate suspicious activity monitoring and reporting systems. Although OFAC is not a part of BSA, BSA examiners typically evaluate the effectiveness of the financial institution’s OFAC compliance program during the exam.

The entire text of the USA PATRIOT Act can be found at FinCEN’s website: www.fincen.gov/hr3162.pdf. We recommend that you review it thoroughly, as well as its regulations, with your legal counsel.

Penalties

It is important to point out that institutions continue to find themselves in violation of BSA regulations. Failures frequently result from inadequate or absent components within compliance programs in particular, risk analysis and SARs, failure to designate a compliance officer and a lack of adequate training on the compliance program requirements, policies and procedures. As a whole, regulators note that one of the primary challenges they face in providing guidance to financial institutions is the general lack of understanding about risk management across the industry.
Those who violate the regulations are subject to severe penalties. Bank directors, officers and employees may suffer suspension or removal from their positions, among other penalties. Institutions that participate in money laundering or criminally violate the BSA can potentially suffer penalties including a loss of their bank charters and deposit insurance.

While penalties for failing to comply with the BSA can be severe, a more detrimental impact can be damage to the financial institution’s reputation. Because the success of financial institutions is largely tied to public trust, allegations (whether factual or not) of involvement with money laundering or terrorist financing can dramatically impact an organization’s bottom line. The significance of actions required under the BSA therefore expands beyond compliance; they show good corporate citizenship and demonstrate a commitment by the organization to prevent criminal activity within its operations.

Sources
3. Ibid., p. 19-23.
5. Ibid., p. 24.
11. The agencies include the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the United States Department of the Treasury through the Financial Crimes Enforcement Network.
13. Ibid., p. 25109.
18. Accounts not meeting this threshold value, although not subject to §312, are still subject to internal controls and risk-based due diligence included in the financial institution’s general AML program.
19. HR3162, p. 86-87.
22. Ibid., p. 89-92.
23. HR3162, p. 93-94.
For more information:
Call 800.949.2732 or visit lexisnexis.com/risk/financial-services

About LexisNexis® Risk Solutions
LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced scoring analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.