

Nevada Registered Agent Association



BEST PRACTICES RECOMMENDATIONS to Prevent the Exploitation of Nevada Business Entities for Criminal Activities, and for the Protection of the Nevada Registered Agent Industry.

Adopted and Approved by unanimous vote of the Nevada Registered Agent Association membership at a meeting held on September 25, 2008, at Carson City, Nevada.

1. INTRODUCTION

- 1.1. INTENT. The Nevada Registered Agents Association (“NRAA”) has developed these Best Practice Recommendations to address legitimate concerns regarding the use of our products and services to facilitate money laundering, tax evasion or the financing of terrorist or other illegal activities. It is our intention, through the adoption of these Best Practices, to proactively minimize the abuse of Nevada entities for these illegal purposes.
- 1.2. LIMITED LIABILITY IS ESSENTIAL. The United States’ commercial engine depends upon the use of business entities that afford entrepreneurs and ongoing owners the protection of limited risk and liability. The advantages of limited liability organizations have been time-tested, and are critical to the growth and development of the U.S. economy. Sophisticated, legitimate business planners routinely use multiple business entities created in jurisdictions that provide the specific benefits and advantages they seek for protection from liability, achieving flexibility and the consistent application of laws.
- 1.3. NEVADA PUBLIC POLICY. In Nevada, the Secretary of State, the Legislature, the Nevada Bar Association, and the NRAA have worked diligently and cooperatively to keep Nevada a highly desirable location to attract and form business entities. Nevada provides for the timely and efficient formation of legal entities, such as corporations, limited liability companies, limited partnerships and other business entities. The culmination of these public policy efforts facilitates business transactions and the timely formation of new companies to take advantage of emerging business opportunities. With over 300,000 active business

entities on the records of the Secretary of State today, as well as an estimated 70,000 new entities formed here each year, Nevada's company formation agent industry brings millions of dollars in much needed revenue and related economic activity to the State.

- 1.4. **POTENTIAL FOR ABUSE.** Nevada has been singled out as potentially attracting those individuals who would engage in abusive practices, due, in large part to its efficient filing practices, business-friendly laws and a highly visible company formation agent industry. NRAA members make up a large part of this industry in Nevada. NRAA members facilitate commerce by assisting lawyers, individuals, and businesses in forming legal entities for legitimate purposes.
- 1.5. **AREAS OF ABUSE.** While almost all business entities are created to further a lawful purpose, some are not. The Congress of the United States; law enforcement; the intelligence community; and international organizations, such as the Financial Action Task Force, have each identified the potential for the abuse of legal entities to facilitate:
 - 1.5.1. Money laundering,
 - 1.5.2. Terrorist financing,
 - 1.5.3. Tax evasion; and,
 - 1.5.4. Violation of U.S. economic sanctions laws.
- 1.6. **GOALS AND OBJECTIVES.** Like other industry associations such as the Association of Registered Agents and the National Public Records Research Association, NRAA members believe that the development and implementation of risk-based due diligence programs pursuant to a set of industry-wide best practices ("Best Practices Recommendations") will provide the guidance needed to:
 - 1.6.1. **EXERCISE SOUND JUDGMENT** when engaging in business with various individuals and entities;
 - 1.6.2. **PROVIDE A FRAMEWORK FOR MONITORING** ongoing relationships with our customers;
 - 1.6.3. **PROMOTE COMPLIANCE** with applicable federal and state laws governing the conduct of business with sanctioned individuals, entities and jurisdictions;
 - 1.6.4. **SERVE AS RESPONSIBLE CITIZENS** in the effort to prevent criminal and terrorist activity;
 - 1.6.5. **SUPPORT THE EFFORTS OF THE NEVADA SECRETARY OF STATE** and State Legislature to promote the unique benefits of forming a business in Nevada to the legal community and small business/entrepreneurs;

- 1.6.6. DISCOURAGE BUSINESS OR MARKETING PRACTICES that promote Nevada in a manner that might encourage use of Nevada entities as a vehicle to conduct illegal activities;
 - 1.6.7. ESTABLISH RECOMMENDATIONS for, and assess the relative risks of, services provided by NRAA members;
 - 1.6.8. REINFORCE THE VALUE and importance of the role and responsibilities of the Company Formation and Registered Agent Industry in this State; and,
 - 1.6.9. PROTECT THE NEVADA REGISTERED AGENT INDUSTRY from damage that could result from abusive practices.
- 1.7. RISK-BASED COMPLIANCE. To achieve these goals, the NRAA recommends that members should adopt the Best Practices recommended herein in order to identify the level of risk they face from areas of abuse. Each member should assess their respective risk, based upon an analysis of their marketing practices, product/service mix, clientele, and the geographies in which they operate, as provided herein. Each member should develop appropriate internal controls to address findings of their risk assessment, which should include policies, plans, and procedures to manage these risks. The result of this process will be a risk-based compliance program for each NRAA member.
- 1.8. ONGOING COMPLIANCE. These Best Practices Recommendations set forth a series of steps each member should take on an ongoing basis. Therefore, each party should recognize that fulfilling these best practices is an ongoing process and continuing responsibility.
- 1.9. APPLICABILITY OF RECOMMENDATIONS. The NRAA recognizes that each member may offer a somewhat unique product/service mix, may target different types of leads from different lead sources in their marketing, and may market in different geographic areas. Each member should implement these Best Practices Recommendations based upon its specific circumstances. To the extent that there is any conflict between these Best Practice Recommendations and any applicable laws or regulations, priority must be given to existing laws and regulations.

2. BEST PRACTICES RECOMMENDATIONS

2.1. Recommendations on Risk Assessment

2.1.1. PERIODIC ASSESSMENT. Each NRAA member should conduct regular and periodic assessments to determine the degree of risk of conducting business or facilitating transactions with individuals or entities that would use U.S. business entities to conduct criminal activities and individuals and entities that are the target of U.S. economic sanctions laws. Each risk assessment should analyze risk from the perspective of

2.1.1.1. The marketing practices of the member;

2.1.1.2. The products and services offered;

2.1.1.3. The nature and characteristics of the company's customers;

2.1.1.4. The channels through which customers are referred, and;

2.1.1.5. The geographic areas the company serves.

2.1.2. FREQUENCY. Each member should base the frequency of these assessments on the nature of the risk discovered in previous assessments.

2.1.3. CUSTOMER RISK. Determining the potential risk of money laundering, terrorist financing or other illegal activity posed by a customer or a category of customers is critical to the development of an effective risk program. Members should determine if it is, or reasonably should be, aware of individual customers or customer segments whose activities may indicate a higher risk.

2.1.4. PRODUCT RISK. An overall risk assessment should also include determining the potential risk presented by products and services offered by a member. Determining the risks of products and services should include the consideration of such factors as:

2.1.4.1. FINANCIAL INTERMEDIARIES: Financial Services where members, acting as financial intermediaries, actually handle the receipt and transmission of cash proceeds through accounts they actually control in the act of closing a business transaction; and,

2.1.4.2. CONCEALED OWNERSHIP: Services to conceal beneficial ownership from competent authorities.

2.1.5. OTHER RISK FACTORS. Each member should address the following special topics during the risk assessment phase; even if only to verify and document that the topic does not apply to their business.

- 2.1.5.1. USE OF E-COMMERCE and other technologies favoring anonymity: Assess the adequacy of the company's policies, plans and procedures to identify the client who uses a technological interface to transact business.
- 2.1.5.2. TRUST AND ASSET MANAGEMENT SERVICES: Assess the adequacy of the company's policies, plans and procedures to identify any client who deposits money or other property with the company. The assessment should take into consideration factors such as whether the provision of such services is subject to federal or state anti-money laundering program requirements and whether the company is subject to examination for compliance with such requirements.
- 2.1.5.3. RECORDS RETENTION POLICIES: Assess the adequacy of the company's records retention policies that safeguard information for a reasonable period of time, consistent with Section 2.10, herein.
- 2.1.5.4. NOMINEE OFFICER AND DIRECTOR SERVICES: Assess the adequacy of the company's policies, plans and procedures to manage the risks associated with providing nominee services consistent with Section 2.8, herein.

2.2. Recommendations on Written Policies

- 2.2.1. FORMAL POLICIES. Based upon the analysis conducted during the risk assessment phase, each NRAA member should develop formal, written policies, plans and internal controls and procedures to mitigate identified risks. These formal policies should address the specific actions each company will take to mitigate identified risks and establish the necessary customer due diligence, customer identification, employee training and records retention programs related to these best practices.
- 2.2.2. INTERNAL CONTROL FACTORS. Members should understand that the nature and extent of their internal controls depends upon several factors, including:
 - 2.2.2.1. The volume of business,
 - 2.2.2.2. The variety of services offered,
 - 2.2.2.3. The customer profile,
 - 2.2.2.4. Assessment of risk associated with each service offering, and
 - 2.2.2.5. The extent to which the member deals directly with the entity and its owners rather than through attorneys, accountants and other intermediaries.

2.2.3. INTERNAL CONTROLS. Elements of internal controls could include:

- 2.2.3.1. Focus on services, customer profiles, and geographic location of customers;
- 2.2.3.2. Provide for regular review of risk assessment based upon the above profile and location data;
- 2.2.3.3. Focus on meeting all regulatory record keeping and reporting requirements;
- 2.2.3.4. Provide updates to regulatory changes;
- 2.2.3.5. Incorporate compliance into job descriptions and performance evaluations of appropriate personnel, and
- 2.2.3.6. Provide appropriate training to all staff.

2.3. Recommendations on Training

2.3.1. TRAINING PROGRAM. Each NRAA member should implement a training program to educate employees as to their role in the fight against money laundering, tax evasion, financing of terrorist activities, and in the enforcement of United States Economic Sanctions Programs. Employers should teach their employees their company's policies and procedures to report suspicious activities based on their relative job description, and the identity of the person within their company designated to receive such reports. Employers should also direct their employees to report suspicious activity to the proper person.

2.3.2. TRAINING CONSIDERATIONS. In developing an employee training program, each NRAA member should consider such factors as: who in the organization will provide training, the scope of training, level of training materials, as well as methods of training. (e.g. internet, self-training and testing, group training etc.)

2.3.3. TRAINING CONTENT. Each NRAA member shall determine the appropriate content for such training. The NRAA recommends the following topics be included in any such program:

- 2.3.3.1. Registered Agent requirements under Title 7 of the Nevada Revised Statutes;
- 2.3.3.2. Payday Lender Compliance, as outlined in Section 2.9, herein;
- 2.3.3.3. State and Federal Laws: Money Laundering and Terrorist Financing, including FATF and OFAC requirements, as outlined in Section 2.5 herein;
- 2.3.3.4. Assessing Customer Risk/Customer Due Diligence, as outlined in Sections 2.1 and 2.4, herein;

- 2.3.3.5. Product and Service Recommendations, including, but not limited to, those outlined in Section 2.8, herein;
- 2.3.3.6. Identifying Potentially Suspicious Activities, as outlined in Section 2.6, herein; and,
- 2.3.3.7. Marketing Practices, as outlined in Section 2.7, herein.

2.4. Recommendations on Customer Identification Programs

- 2.4.1. CUSTOMER DEFINITION. For the purposes of this document, “customer” is defined as the purchaser of services. If a product or service is requested by an individual acting on behalf of an entity, then the entity is deemed to be the customer; if such individual is acting on his or her own behalf, the individual is deemed to be the customer.
- 2.4.2. CUSTOMER IDENTIFICATION PROGRAM (CIP). For the customers of its corporate formation and registered agent services, each NRAA member should implement a CIP and any required due diligence to support that program. The application of the CIP should be in proportion to the level of risk associated with a particular product, service, customer or transaction.
- 2.4.3. DUE DILIGENCE. The CIP should consider the nature or source of the customer, including the nationality of individuals or businesses, prior knowledge of customers, degree of direct contact, referral, and whether customer contact takes place through an intermediary etc. Each member should determine the amount of customer information necessary to adequately identify the customer. With regard to customer due diligence, each NRAA member should consider, based upon risk, the appropriate level of due diligence required (e.g. screening against sanctions lists, required documentation, background investigation reports, etc.)

2.5. Recommendations on OFAC Compliance

- 2.5.1. SPECIALLY DESIGNATED NATIONALS LIST. Each NRAA member should implement procedures to screen the names of customers against the Specially Designated Nationals List (“SDN List”).
- 2.5.2. PROHIBITED PERSONS. The U.S. Department of the Treasury’s Office of Financial Asset Control (OFAC) does not mandate what type of compliance program company formation agents must have; however, this task is critical because allowing any person or entity listed on the SDN list or from a sanctioned country to incorporate in the United States is prohibited. If a member has reason to be

suspicious that a potential customer is either a Specially Designated National or affiliated with a sanctioned country, OFAC recommends requesting further information to determine whether doing business with the applicant constitutes a violation of federal law.

2.5.3. TREASURY REGULATIONS. Members can obtain additional information about this requirement from the U.S. Treasury's publication "*Foreign Assets Control Regulations for the Corporate Registration Industry*" (provided as an exhibit to this Best Practices document). The most recent copy of the Specially Designation Nationals List can be obtained on the U.S. Department of the Treasury website at <http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf>.

2.6. Recommendations on Identifying Potentially Suspicious Activities

2.6.1. CONTEXT. NRAA members do not assume the activities listed below in Section 2.6.4 to be inherently illegal or unethical, however, absent a context in which reputable clients conduct these activities for reasonable purposes, they could indicate a pattern of behavior that members should identify as potentially suspicious.

2.6.2. INTERNAL SYSTEMS. NRAA members should implement internal systems that could identify potentially suspicious client activities as listed below, with an appropriate response for each identified circumstance. Members who become aware of the practices listed below should respond for their own protection, as well as for the protection of the industry, in a manner appropriate for the circumstances.

2.6.3. RESPONSE. The member's response to a client involved in potentially suspicious activities could include, but are not limited to:

- 2.6.3.1. Bringing the situation to the attention of a supervisor;
- 2.6.3.2. Increased due diligence by the member;
- 2.6.3.3. Resignation as registered agent;
- 2.6.3.4. Reporting to the Secretary of State or appropriate law enforcement agencies, etc.

2.6.4. POTENTIALLY SUSPICIOUS ACTIVITIES. Potentially suspicious activities can include, but are not limited to:

- 2.6.4.1. PATTERNS OF AMENDMENT.
 - 2.6.4.1.1. Systematically or frequently amending, increasing or decreasing authorized shares. These activities could be indicative of securities violations or investor fraud.

- 2.6.4.1.2. Frequent entity name changes or amended officers/director lists, or the systematic or frequent activity by a single client making these changes for multiple entities. This could indicate that the individual is using the entity or entities for any number of illicit or illegal purposes, or that the entity or individual is attempting to fraudulently evade legal process or engage in corporate identity theft.
- 2.6.4.2. UNCONNECTED REINSTATEMENT. Reinstatement of delinquent or revoked entities where there is no evident connection between the entities and the client; or the reinstatement of multiple revoked entities. This could indicate corporate identity theft.
- 2.6.4.3. FREQUENT AGENT CHANGES. Systematic, frequent or the regular changing of registered agent/registered office. This could be indicative of non-compliance with requirements to provide information necessary for the agent to “know your client” or other required records.
- 2.6.4.4. UNUSUAL MODIFICATIONS. Unusual patterns of document modifications.
- 2.6.4.5. NON-PAYMENT. Using non-sufficient funds checks, invalid credit cards or fraudulent charge-backs, especially for entity formation or purchasing existing corporate shells. This may indicate a high-risk pattern of fraud by the client.
- 2.6.4.6. CORPORATION SOLE. Using a corporation sole.
- 2.6.4.7. MANIFESTLY SUSPICIOUS ACTIVITIES.
 - 2.6.4.7.1. Obtaining any direct knowledge of manifestly suspicious or illegal business activities or practices; or
 - 2.6.4.7.2. Obtaining any direct knowledge that the client is not reputable or is acting suspiciously unreasonable in the given circumstances.

2.7. Recommendations on Marketing Practices

- 2.7.1. CONTEXT. The Nevada Registered Agent Association discourages business practices or marketing efforts that promote or encourage the use of Nevada business entities as a vehicle to conduct illegal activities. NRAA members recognize that the general propensity of individuals within a member’s client database to use Nevada entities for illegal purposes in a manner that may cast a negative light on our industry as a whole or attract the scrutiny of law enforcement, tax authorities and political leaders, can be a reflection of the business and marketing practices of that member. Unethical or

problematic business and marketing practices have potential to result in an unethical or problematic client base.

2.7.2. DISCOURAGED PRACTICES. The Best Practices standard for NRAA members in the area of marketing strongly discourages strategies that encourage the promotion, discussion or sale of products that involve:

2.7.2.1. DISGUISED OWNERSHIP. Disguised ownership can be used to facilitate underreporting of income, tax non-compliance, money laundering, financial crimes and potentially terrorist financing. Included in this category are all forms of anonymous or nominee ownership.

2.7.2.2. TAX HAVENS. The term "tax haven", though it does not technically communicate inherently illegal activities, may infer an attitude or philosophy that encourages financial non-compliance.

2.7.2.3. IRS INFORMATION SHARING. The representation to the public regarding Nevada's policies or relationships toward the Internal Revenue Service has potential to attract the interest of individuals who are more likely to be tax non-compliant.

2.7.2.4. OFFSHORE COMPARISONS. Comparing Nevada entities with notorious offshore jurisdictions communicates the concept that Nevada can be used in a manner that encourages the very type of activity that has resulted in significant negative publicity, black-listing, non-compliance, and even criminal prosecutions of individuals using those jurisdictions.

2.7.2.5. CORPORATION SOLE. The IRS has targeted corporation sole abuse for many years. Participants apply for incorporation under the pretext of being an overseer of a one-person religious organization with the idea that this entitles the individual to exemption from federal income tax.

2.8. Recommendations on Nominee Officer/Director Services

2.8.1. DEFINITION: For the purposes of this section, a nominee is defined as a natural person who is designated and appointed to act as a temporary substitute for an officer/director or manager for a term or anticipated term of less than the term specified in the bylaws or operating agreement of the company; or for a term of less than six months if no term is designated. The nominee provides the valuable service of protecting clients from potential identity theft, fraud, or other scams that utilize public record documents made available by the Nevada Secretary of State. The definition of a nominee *does not* include individuals who are hired to engage in any ongoing

management or operations of the company. *Nominee services are not provided for the purpose of disguising ownership.*

2.8.2. SCOPE OF SERVICES: Nominee officers/directors or managers execute limited acceptance on behalf of the entity. The nominee is authorized to execute and file official state documents for the purpose of maintaining technical compliance with Nevada statutes in accordance with a formal contract between the parties, as outlined in Best Practice Standard item 2.8.3.6, referenced below.

2.8.3. BEST PRACTICE RECOMMENDATIONS:

2.8.3.1. DOCUMENTATION. The nominee shall document the complete paper trail of all appointments, acceptances, and resignations for entities they have served in their capacity as a nominee.

2.8.3.2. RECORD RETENTION. The nominee shall retain all documentation related to individuals and entities served in their capacity as a nominee for a period of three years after the final termination of nominee services.

2.8.3.3. LIMITATIONS. The limited acceptance of the nominee should not allow for conducting any regular day-to-day business on behalf of the entity, including banking, facilitating transactions, executing contracts and agreements on behalf of the entity, or assuming fiduciary responsibility for corporate formalities (other than those incidental to providing nominee service), acquiring Taxpayer Identification Numbers (TIN) using the nominee's personal information or signing tax returns. Internal corporate formalities, TIN applications and tax returns should be executed by the permanent officers/directors/managers.

2.8.3.4. KNOW-YOUR-CLIENT. The nominee provider should institute "know-your-client" systems and practices to verify and document the identity and location of each client, and the business purpose of every entity being served. The nominee should check all clients against the SDN List, and should conduct reasonable, additional background checks as necessary to reduce the risk of clients abusing the nominee service for illegal purposes.

2.8.3.5. CONTRACTS. Nominee services should be provided on a contract basis, which should clearly outline the limitations of the service, the responsibilities of the client, and the terms and conditions of the nominee relationship, including the "know-your-client" standards in effect at that time.

2.8.3.6. SEPARATION OF RISK. The nominee services should be provided through an entity that is separate and distinct from the entity or individual that provides registered agent services.

2.8.3.7. **INTERNATIONAL RESTRICTION.** Nominee services should not be provided for non-resident aliens or for entities formed in international jurisdictions.

2.8.3.8. **LICENSED OR REGULATED ACTIVITIES.** Nominee services should not be provided to entities engaged in activities that require specialized or professional licensing.

2.9. **Recommendations on Payday Lender Compliance**

2.9.1. **STATUTORY REQUIREMENT.** NRAA members providing services other than those enumerated in NRS 77.410 should conduct periodic assessments to identify if it, or any subsidiary or sister company, knows whether it represents any client that is providing services to the public involving:

2.9.1.1. Deferred deposit loans,

2.9.1.2. High interest loans,

2.9.1.3. Title loans,

2.9.1.4. Check cashing services, or

2.9.1.5. Installment loans.

2.9.2. **IMPLEMENTATION.** Each NRAA member should adopt policies and procedures that comply with NRS 77.410 to provide for the verification of licensing with the Nevada Division of Financial Institutions that can be implemented in the event that the member identifies that it represents a client involved in any of the above-listed activities. Members should avoid providing transactional support, such as preparing banking deposits, etc. for clients involved in these activities.

2.10. **Recommendations on Record Retention**

2.10.1. **DOCUMENTATION.** Each NRAA member should retain written records documenting:

2.10.1.1. **ASSESSMENT FINDINGS:** The findings of each member's risk assessment overview completed during each periodic risk assessment phase

2.10.1.2. **POLICIES:** Policies, plans and procedures adopted to mitigate risks identified during the risk assessment phase

2.10.1.3. **TRAINING:** Training materials produced, and training conducted in furtherance of polices, plans and procedures to mitigate risks.

2.10.1.4. STATUTORY REQUIREMENTS: Documents and client records as required to be maintained by Title 7 of the Nevada Revised Statutes.

2.10.1.5. OFAC: Documentation of policies and procedures to comply with the OFAC regulations for the Corporate Registration Industry and any correspondence related thereto.

2.11. Recommendations on Compliance

2.11.1. MANAGEMENT OVERSIGHT. Each NRAA member should identify, in writing, a person or persons, responsible for managing the company's programs to implement these Best Practices Recommendations. This person should hold sufficient seniority within the company's management structure to be able to carry out the policies.

2.12. Recommendations on Implementation

2.12.1. INDIVIDUAL ADOPTION. Each NRAA member should review and formally approve and accept these Best Practices Recommendations pursuant to its own executive management decision making process and should document their adoption and acceptance as part of the company's records.

ADDENDUM 1: OFAC REGULATIONS



FOREIGN ASSETS CONTROL REGULATIONS FOR THE CORPORATE REGISTRATION INDUSTRY

Why?

This brochure provides the corporate registration industry with information about the Specially Designated Nationals and Blocked Persons list (SDN list) of the Office of Foreign Assets Control (OFAC) and other aspects of U.S. sanctions programs. In response to the increased nationwide effort to prevent terrorists, terrorist supporters, narcotics traffickers, and other sanctioned parties from using the U.S. financial system, it is critical that the corporate registration industry implement steps to identify sanctioned parties in order to prevent their incorporation in the United States.

All organizations involved in the corporate registration process need to understand OFAC regulations. Undertaking any type of business or financial transaction with a sanctions target is illegal under federal law and the industry can make an important contribution to the achievement of national security goals by identifying sanctioned targets in order to block their ability to use the U.S. financial system or do business in the United States.

The following example illustrates what can happen if OFAC compliance is ignored: During the 1990s, the U.S. Government placed comprehensive sanctions on the Federal Republic of Yugoslavia (Serbia & Montenegro) for its role in fostering war in the Balkans region. The sanctions prohibited U.S. persons from doing business with individuals or entities located in Yugoslavia and prohibited Yugoslavians from using the U.S. financial system. While the sanctions program was still in place, a Serbian company submitted an application to a U.S. business filing company and was incorporated under a new name in the United States. The U.S. entity was then used by the Serbian company to open seemingly legitimate bank accounts and to transfer money through the United States. Because the business filing company's employees were not trained on OFAC sanctions policies, the company not only permitted a sanctions target to do business in the United States, it also violated federal law.

About OFAC

Economic sanctions are used by the U.S. government to prevent targeted countries, entities, and individuals from, among other things, accessing the U.S. financial system for purposes that are contrary to U.S. foreign policy and national security objectives. OFAC exercises this authority based on a number of different statutes, including:

- Trading With the Enemy Act (TWEA), 50 U.S.C. App. §§ 1-44
- International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701-06
- Iraqi Sanctions Act (ISA), Pub.L. 101-513, secs. 586-586J, 104 Stat. 2047-55
- United Nations Participation Act (UNPA), 22 U.S.C. § 287c
- International Security and Development Cooperation Act (ISDCA), 22 U.S.C. 2349 aa-8 and aa-9
- Cuban Democracy Act (CDA), 22 U.S.C. § 6001-10
- Cuban Liberty and Democratic Solidarity (LIBERTAD) Act, 22 U.S.C. 6021-91
- Antiterrorism and Effective Death Penalty Act, 8 U.S.C. 1189, 18 U.S.C. 2332d, and 18 U.S.C. 2339B

- Foreign Narcotics Kingpin Designation Act, 21 U.S.C. 1901-1908, 8 U.S.C. 1182
- The Trade Sanctions Reform and Export Enhancement Act (TSRA), 22 U.S.C. 7201-11

These statutes often involve declarations of "national emergency" by the President.

Sanctions Programs

As of October 2004, OFAC administered and enforced comprehensive sanctions programs involving three countries: Cuba, Iran, and Sudan. Unless authorized by OFAC, no U.S. individual or entity can do business with individuals or entities (including government institutions) in those countries, or individuals or entities acting for or on behalf of those countries. For example, incorporating an entity on behalf of a resident of Iran, Cuba, or Sudan would be prohibited. In addition, when the Cuba program is involved, U.S. individuals are also prohibited from doing business with any Cuban national regardless of where he or she resides unless that person is a citizen or permanent resident alien of the United States or is otherwise authorized by OFAC. OFAC also enforces sanctions regimes regarding: the Western Balkans, Burma (Myanmar), diamond trading, Iraq, Liberia, narcotics trafficking, North Korea, the proliferation of weapons of mass destruction, Syria, terrorism, and Zimbabwe. To read about the specifics of each sanctions program and to learn about recent changes to our programs, please visit: www.treas.gov/ofac

Specially Designated Nationals and Blocked Persons List

OFAC has identified and officially "designated" numerous foreign agents and front organizations, as well as terrorists, terrorist organizations, and narcotics traffickers, on its SDN list, which contains over 5,000 variations on names of individuals, governmental entities, companies, and merchant vessels located around the world. To ensure that illicit transactions involving targeted countries and SDNs are not processed, many U.S. banks and corporations are using sophisticated "interdiction" software, developed by the private sector, to flag questionable transactions for review. If such software flags an item as a potential match to OFAC's SDN list, certain "due diligence" steps outlined in this brochure should be taken to verify whether it is an actual match before contacting OFAC or taking action with regard to the match.

Who Must Comply?

All U.S. persons (including individuals and entities) are responsible for ensuring that they do not undertake a business dealing with an individual or entity on the SDN list. U.S. persons are:

- All U.S. citizens and permanent residents,
- All persons located in the United States,
- Any business organized under U.S. law, including U.S. branches and representative offices of foreign companies and overseas branches of U.S. companies, and

- In the case of the Cuba and North Korea programs, non-U.S. subsidiaries of U.S. companies.

Penalties for Noncompliance

Depending on the program involved, criminal violations of the statutes administered by OFAC can result in penalties ranging from \$50,000 to \$10,000,000 and/or up to 30 years imprisonment for willful violations. OFAC also has authority to impose civil penalties of up to \$1,075,000 per violation depending on the sanctions program.

What does "Compliance" Entail?

OFAC does not mandate what type of compliance program a U.S. organization should have. Every organization has a different level of risk that must be assessed to determine the best way to ensure that it does not do business with a sanctions target. For entities in the corporate registration industry, this task is critical because allowing a sanctions target to incorporate in the United States is prohibited and provides access to the U.S. financial system and the ability to move money for purposes contrary to national security objectives.

Because the corporate registration process is highly decentralized and governed by different state laws, some applications may contain minimal or incomplete information on the parties requesting incorporation. If you have reason to be suspicious that an applicant is either a Specially Designated National or affiliated with a sanctioned country, OFAC recommends requesting further information to determine whether doing business with the applicant constitutes a violation of federal law.

How to Determine if a Registration Application Contains an Exact Match to the SDN List

Interdiction software is a tool to help identify potential matches with OFAC's SDN list. Inevitably, there will be "false positives" with the use of this software. Therefore, certain "due diligence" steps should be taken to ensure that a "hit" is a "good hit" (i.e., to determine whether the individual or entity on the application is indeed on the SDN list). The following is a guide on how to determine if you have a "good hit" when evaluating potential matches against the SDN list:

1. Is the "hit" or "match" listed on the incorporation application against OFAC's SDN list or targeted countries, or is it "hitting" for some other reason (i.e., Control List or PEP, Non-Cooperative Countries and Territories, Canadian Consolidated List (OSFI), World Bank Debarred Parties, Blocked Officials File, or government official of a designated country), or can you tell what the hit is?

- If the name is hitting against OFAC's SDN list or targeted countries, continue to Step 2 below.
- If it is hitting for some other reason, you should contact the "keeper" of whichever other list the match is hitting against. For questions about: (1) The Denied Persons List and the Entities List, please contact the Bureau of Industry and Security at the U.S. Department of Commerce at 202-482-4811, (2) The FBI's Most Wanted List or any other FBI-issued watch list, please see the Federal Bureau of Investigation's website at www.fbi.gov/contact/fo/fo.htm, (3) The Debarred Parties List, please contact the Office of Defense Trade Controls at the U.S. Department of State, 202-663-2700, (4) The Bank Secrecy Act and the USA PATRIOT Act, please contact the Financial Crimes Enforcement Network (FinCEN) at 1-800-949-2732.
- If you are unsure whom to contact, please contact the provider of the interdiction software that told you there was a hit.
- If you cannot tell what the hit is, you should contact the provider of the interdiction software which told you there was a hit.

2. Now that you have established that the hit is against OFAC's SDN list or targeted countries, you must evaluate the quality of the hit. Compare the name of the individual with the name on the SDN list. Is the name on the SDN list a vessel or a company rather than an individual (or vice-versa)? Is the name on the SDN list a male's name whereas your applicant is a female?

- If yes to either question, you do not have a valid match.*
- If no, please continue to Step 3 below.

3. How much of the SDN's name is matching against the name on your application? Is just one of two or more names matching (i.e., just the last name or just the first name)?

- If yes, you do not have a valid match.*
- If no, please continue to Step 4 below.

4. Compare the complete SDN entry with all of the information you have on the matching name on your application. An SDN entry often will have, for example, a full name, address, nationality, passport, tax ID or credula number, place of birth, date of birth, former names and aliases. Are you missing a lot of this information for the name on your application?

- If yes, go back and get more information and then compare your complete information against the SDN entry.
- If no, please continue to Step 5 below.

5. Are there a number of similarities or exact matches?

- If yes, please call the hotline at 1-800-540-6322.
- If no, you do not have a valid match.*

** If you have reason to know or believe that allowing this person to do business in the United States would violate any of the Regulations, you should call the hotline and explain this knowledge or belief.*

Staying Up-to-Date

Whenever there is an update to any of OFAC's information, it is quickly made available electronically via many different sources:

All of OFAC's program brochures, as well as SDN information, are available free in downloadable camera-ready Adobe Acrobat® ".PDF" format over the Treasury Department's World Wide Web Server. OFAC's Home Page is located at www.treas.gov/ofac. The website also contains a self-extracting ASCII file of the SDN list in DOS, delimited, fixed-field, and country-specific versions, and access to all OFAC-related Executive Orders, U.N. Resolutions, statutes, regulations, and the Code of Federal Regulations as well as to brochures in ASCII format.

All of OFAC's forms, including its Annual Report on Blocked Property, Cuban Remittance Affidavit, and license applications are electronically available on the site. Whenever there is a change involving urgent information requiring immediate implementation, the [DATE] changes on the face of the primary Page; users can automate their compliance by structuring their Internet connection to use a Web browser to watch for that date change, check a "Bulletin" file to get the details about changes, and download OFAC's latest information for incorporation, for example, into interdiction software.

There are two separate email subscription services on the site, one called a "Financial Operations Bulletin" and the other a "What's New" notice. Financial operations bulletins are geared toward the financial operations community, while "What's New" notices are geared toward the general public (including exporters and importers, practicing attorneys, and researchers). Generally speaking, those in the operations areas of banks, brokerage houses, and other financial service providers do not require the level of detail and wealth of information provided in no-

tices to the general public. Instead, they are primarily interested in changes directly impacting their day-to-day operations, such as updates to OFAC's listing Specially Designated Nationals and Blocked Persons. All "What's New" notices to the general public also contain information from OFAC's financial operations bulletins.

OFAC operates a free automated fax-on-demand service, which can be accessed 24 hours a day, seven days a week, by dialing 202/622-0077 from any touch-tone

phone and following voice prompts. OFAC documents kept up to date on the system include program and general brochures, listings of Specially Designated Nationals and Blocked Persons, including changes to the listings, licensing guidelines, and *Federal Register* notices (even those filed but not yet printed in the *Federal Register*). The "Index of Available Documents" is date-specific.

ADDENDUM 2: NRS 77.410

NRS 77.410 Registered agent required to verify licensure of entity under certain circumstances. [Effective July 1, 2008.]

1. If a registered agent knows or reasonably should know that the entity for which he is the registered agent engages in any business activity that is regulated pursuant to chapter 604A or 675 of NRS and the registered agent or a subsidiary or affiliate of the registered agent performs any service for the represented entity other than:

(a) Delivering documents for filing to state or local governmental entities;

(b) Forwarding unopened mail;

(c) Any service described in NRS 77.400;

(d) Accounting services incidental to the formation of the entity for which he serves as registered agent provided in accordance with chapter 628 of NRS; or

(e) Legal services incidental to the formation of the entity for which he serves as registered agent if he is an attorney who is licensed to practice law in this State or performs such services under the supervision of an attorney who is licensed to practice law in this State, the registered agent shall verify with the Division of Financial Institutions of the Department of Business and Industry that the represented entity is licensed pursuant to chapter 604A or 675 of NRS, as applicable.

2. If a registered agent determines pursuant to subsection 1 that the represented entity is not licensed as required pursuant to chapter 604A or 675 of NRS, the registered agent shall notify the Commissioner of Financial Institutions.

3. A registered agent who accepts an appointment to act as the registered agent for a represented entity whom the registered agent knows or reasonably should know engages in business activities which are regulated pursuant to chapter 604A or 675 of NRS shall not perform any financial transactions on behalf of the represented entity in his capacity as registered agent.

(Added to NRS by 2007, 2637, effective July 1, 2008)