



Nevada Registered Agents 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

1. INTRODUCTION

1.1. INTENT. The Nevada Registered Agents Association ("NRAA") has developed these Best Practice Recommendations to minimize, 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, 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 STANDARDS for, and assess the relative risks of, services provided by NRAA members, and
- 1.6.8. REINFORCE THE VALUE and importance of the role and responsibilities of the Company Formation and Registered Agent Industry in this State.
- 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 must 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 money laundering or terrorist financing risks 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. These activities include the following:

2.1.3.1. UNUSUAL CIRCUMSTANCES: Customers conducting their business relationship or transactions in unusual circumstances, such as:

2.1.3.1.1. Significant and unexplained geographic distance between the member and the location of the customer;

2.1.3.1.2. Frequent and unexplained movement of funds between institutions and/or various geographic locations;

- 2.1.3.2. CONCEALED OWNERSHIP: Customers where the structure or nature of the entity or relationship makes it difficult to identify the true owner or controlling interests, such as:
 - 2.1.3.2.1. Unexplained use of corporate structures, and/or use of nominee shares;
 - 2.1.3.2.2. Delegation of authority by the customer through the use of powers of attorney;
 - 2.1.3.2.3. Unexplained relationship between beneficial owners and controllers and accounts signatories;
- 2.1.3.3. CASH INTENSIVE BUSINESSES: Customers using cash (and cash equivalent) intensive businesses including:
 - 2.1.3.3.1.1. Money services businesses (e.g. remittance houses, currency exchange houses, casas de cambio, bureau de change, money transfer agents and bank note traders or other businesses offering money transfer facilities);
 - 2.1.3.3.1.2. Casinos, betting and other gambling related activities;
 - 2.1.3.3.1.3. Businesses not normally cash intensive that generate substantial amounts of cash for certain transactions; and,
 - 2.1.3.3.1.4. Charities and other "not for profit" organizations which are not subject to monitoring or supervision (especially those operating on a multi-state basis);
- 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 must 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 would 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 will consider such factors as: who in the organization to train, 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 Standards, 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 section, "customer" is defined as the primary contact or purchaser of services.
- 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 must 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/index.shtml>.

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 would 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 NRAA "watch list", or;

2.6.3.5. 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. 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 are likely 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. Using entities for the purpose of disguising corporate 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 is likely 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 limited period of time or until permanent officers/directors or managers are duly elected and appointed. 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. *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 only 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 STANDARDS:

- 2.8.3.1. DOCUMENTATION. The nominee must 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) 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. DISCLOSURE. All state filings submitted by a nominee should be identified as such by listing the term "nominee" in parenthesis after the individual's name. Example: John Doe, (Nominee)
- 2.8.3.5. KNOW-YOUR-CLIENT. The nominee provider shall 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 must 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
- 2.8.3.6. CONTRACTS. Nominee services should be provided on a contract basis, which clearly outlines 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.

2.8.3.7. 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.

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

2.8.3.9. 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. Per NRS 77.410, each NRAA member 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 policies, 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.