Disclaimer: *This material is provided as background information for AscdiNatd Members by Association Counsel, Arthur P. Freierman, Esq. It is not intended, nor should it be used, as a substitute for specific legal advice or legal opinions. Governing law may vary from state to state and applicable federal, state and local law should be considered prior to use of this information. Legal counsel is only given in response to inquiries regarding specific situations. For such legal advice, contact your attorney or Arthur Freierman at:*

Arthur P. Freierman, Esq.
45 Rockefeller Plaza, 20th Floor
New York, NY 10111-2099
Tel: 212-332-1616
afreierman@freiermanlaw.com

AscdiNatd
BEST PRACTICES GUIDELINES

Policies and Procedures for Establishing, Maintaining and Monitoring Customer, Vendor and Manufacturer Relationships and Detection of Counterfeit Products

Introduction

The AscdiNatd seeks to maintain and enforce high standards of ethical professional conduct making Membership in the AscdiNatd a recognized mark of experience, integrity and competence. Accordingly, the AscdiNatd promotes adoption by its Members of policies and procedures ("**Best Practices**") that are designed to ensure compliance with all applicable laws and regulations and to detect and prevent, to the best of its ability: fraud, deceptive practices, trafficking in counterfeit goods and money laundering in any dealings with customers and vendors. Members should strive to comply with all relevant laws and rules and regulations promulgated by relevant governmental agencies (collectively, "**Laws and Regulations**"), including the Patriot Act; rules and regulations promulgated for the financial service industry; relevant consumer protection laws; import/export laws, intellectual property laws, and practical applications of sound business practices; all of which will enable Members to maintain these standards and protect themselves from the costs and interference that can result from enforcement by government agencies and claims by manufacturers or other third parties.

A. Designated Compliance Officer

Each Member should designate a **Compliance Officer** who will be responsible for implementing and monitoring the day-to-day operations and internal controls of the Best Practices compliance program. For smaller companies, the Compliance Officer should be a principal of the Member Company; at larger companies, the Compliance Officer should be a principal and/or the chief legal officer of the Company. The Compliance Officer should also be responsible for:

- being aware of changes in relevant Laws and Regulations and understanding in each case how they apply to the Member Company;
- reflecting in the Company's policies and procedures applicable changes in the Laws and Regulations to ensure Best Practices;

- confirming that the Company's continuing education program includes training in compliance with Laws and Regulations to ensure Best Practices;
- evaluating the effectiveness of the program and whether the program should be revised to respond to any apparent or actual weaknesses; and
- reporting to the Board of Directors of the Company any compliance issues.

B. Establishing Customer/Vendor Relationships

Members' efforts to establish Best Practices must extend beyond the internal controls at the Member Company to the relationships it establishes in the industry. The first line of defense is to know your customers and vendors. The majority of your customers/vendors will be companies with which you have had long-standing relationships. Best Practices require due diligence for these customers and particularly new customers/vendors.

1. Documentation

Best Practices should include documentation of customer/vendor background information ("**Account Documentation**"). Account Documentation sets forth the information necessary to establish and verify the bona fide identity of a customer/vendor and to detect any issues that will interfere with Best Practices. Account Documentation should include (where relevant):

- the name of the entity/individual;
- mailing, residential or principal place of business street address;
- list of officers, directors, members or partners;
- the tax identification number of the entity; and
- a signed application that includes representations regarding money prohibited activity, including laundering and trafficking in counterfeit products.

Where the customer purchases equipment from the Member for resale, a current resale certificate should be obtained for all States in which sales occur (generally, where shipments or deliveries are made). Remember, the Member may be required to produce such certificates to State tax auditors to avoid payment of sales tax on the transaction. Resale certificates should be in "blanket" form (i.e., covering all sales to the customer as opposed to one particular sale) and should be updated on at least an annual basis.

An Account Documentation File should be maintained for each customer and vendor either in hard copies or appropriately maintained (and backed up!) digital format.

2. Verification of Customer/Vendor's Identity

Knowing your customers/vendors entails obtaining information as well as verifying it. Members should make a good faith effort to verify:

- Business Name and Street Address. This can often be done quickly by utilizing the Internet as well as telephone and industry directories.
- Tax Identification Number and Organizational Documents. For domestic corporations, this can be accomplished by contacting the Secretary of the State of incorporation. The Compliance Officer should develop methods to verify non-domestic entities.

- Names of Principals and/or Directors. Generally, for domestic public companies, this can be accomplished by checking the Securities and Exchange Commission's Edgar database. For other types of verification methods, contact the Compliance Officer.

Employees should describe in the Account Documentation efforts taken to verify the customer/vendor's identity. In reviewing all Account Documentation for new customers/vendors, the Compliance Officer should confirm that the customer/vendor appears to be bona fide because: (i) they are widely known, (ii) they are sufficiently known to the Member, and/or (iii) the Member has verified the identity by obtaining sufficient, credible information that supports the customer/vendor's identity. The Compliance Officer should evidence the acceptance/acknowledgment of the customer/vendor information by signing off on the Account Documentation File. If he or she does not believe the customer/vendor's identify is bona fide, he or she should request further information from the customer/vendor before accepting any transaction. Where a customer/vendor is reluctant to provide sufficient information, the Compliance Officer shall determine whether it is appropriate to move forward without further documentation.

In addition to the foregoing, all new customers/vendors, as well as current customers/vendors should be screened through appropriate searches. Members should always begin this process with a search of the AscdiNatd database to see if the proposed customer/vendor is cited for any Ethics violation or non-participation in an Ethics proceeding. Another important search is of the Treasury Department's Office of Foreign Assets Control (OFAC) specially designated nationals (SDN) list (available at http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/fuzzy_logic.aspx.) Additional searches should be conducted through other available search engines and, where appropriate, government agencies (e.g., Secretary of State of incorporation, etc.). For example, it could be negligent to begin doing business with an entity without even performing a basic Google search of the company and its principals for background. Database confirmations should be properly documented by placing a copy of the search in the Account Documentation File.

On a yearly basis, the Compliance Officer should re-verify that a vendor or customer is not on the OFAC list and that no criminal activity or Ethics violation by a vendor has occurred. If the prospective customer/vendor refuses to provide any requested information, the account executive should consult the Compliance Officer. Under no circumstances should an account executive move forward with a transaction without proper identification and the Compliance Officer's approval.

Finally, customers and vendors should be provided with a notice of the Member Company's policies regarding product and sourcing (see the AscdiNatd Anti-Counterfeit Policy) and should be required to acknowledge that they will continue to abide by same. A copy of their acknowledgement should also be kept in the relevant Account Documentation File.

3. Prohibited Relationships

a. Persons and Organizations on the OFAC List/U.S. Sanction Program

Executive Order 13224, issued September 24, 2001 ("Order"), freezes the property of and prohibits transactions with persons who "commit, threaten to commit, or support

terrorism." The Order was issued through the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"), which administers and enforces economic and trade sanctions against, among other persons, certain foreign countries and terrorism-sponsoring organizations. OFAC maintains a list of "Terrorists" and "Specially Designated Nationals and Blocked Persons" as well as a list of embargoed countries on its web site located at: www.treas.gov/ofac. Any employee of the Member Company who becomes aware of an attempt by any party on the OFAC list to conduct business with the Member Company should be required to immediately contact the Compliance Officer. The Compliance Officer should then take all steps necessary to cease business (if applicable) and conduct such further investigation/reporting as deemed necessary.

b. Companies Subject to Ethics Violations Under the AscdiNatd Code of Ethics and Non-Participants in Ethics Proceedings

Member Companies should avoid doing business with companies who have been found to have violated the AscdiNatd Code of Ethics and should further vet companies who have declined to participate in the Ethics process where a claim has been filed against them. A listing of ethics violators is available on the AscdiNatd website at https://members.ascdi.com/members/violations and a list of non-member companies who declined to participate in the Ethics process can be found at: https://members.ascdi.com/members/EthicsNonParticipants.

4. Ongoing Compliance Efforts

When possible, every active customer and vendor should be reviewed on an annual basis to confirm compliance with the above guidelines. The Member Company should ensure that AscdiNatd notices regarding Ethics claims and violations and fraud alerts are received by the designated Compliance Officer.

C. MONITORING OF CUSTOMERS/VENDORS AND REPORTING OF SUSPICIOUS ACTIVITY

1. Suspicious Activity Indicators

During the course of a relationship with a customer/vendor, the account executives and the Compliance Officer (or designee) should be wary of certain risk indicators. Examples of customer/vendor suspicious activity indicators are:

- customer/vendor's activity is inconsistent with his or her business or financial background;
- customer/vendor refuses or delays in producing requested information;
- customer/vendor offers gifts or gratuities in excess of traditional limits;
- customer/vendor conducts business under unusual circumstances, at irregular hours, or from unusual locations;
- customer/vendor is seemingly not interested in performance or transaction costs;
- customer/vendor asks an unusual number of questions concerning regulatory reporting requirements, the Member Company's procedures, and how they apply to his/her activities;
- customer/vendor is the subject of significant regulatory or governmental inquiries; or
- customer/vendor is from, or has accounts in, a country identified as a non-cooperative country or territory by the Financial Action Task Force ("FATF"), which is charged with combating money laundering and the financing of terrorism. (see FATF Recommendations at: http://www.fatf-

gafi.org/topics/fatfrecommendations/documents/internationalstandardsoncombatingmoneylaunderingandthefinancingofterrorismproliferation-thefatfrecommendations.html)

2. Internal Monitoring

The Compliance Officer should also undertake a periodic review of Member Company staff's emails and other communications to monitor for suspicious activity of the nature described above. Such review should be part of the Member Company's standard policy regarding e-mails and other use of the Member Company's digital interface and systems and should be clearly described in the Member Company's employment policies. In addition, the Compliance Officer should meet regularly with appropriate departments to solicit information concerning customers, vendors and marketplace intelligence. Finally, employees of Member Companies should be urged to report to the Compliance Officer any activities they deem indicative of illegal or improper activities.

D. ENHANCED DUE DILIGENCE FOR CERTAIN VENDORS/CUSTOMERS

Enhanced due diligence may be necessary regarding vendors/customers that reside in countries having high incidences of corruption and fraud. A useful tool is the yearly rating index published by Transparency International. The Compliance Officer should check ratings and set guidelines for additional due diligence. For example, any vendor/customer who originates from a country having a rating of less than 60 could be subject to enhanced due diligence requiring further investigation/documentation. That may include any of the following:

- Domestic references
- Requesting the names of all their principals to conduct background search
- Request for audited financial statements
- Further research to be done on the company via Internet, etc.
- Other requirements to be determined by the Compliance Officer

E. DETECTION AND PREVENTION OF COUNTERFEIT

The Member Company should establish effective procedures to determine the authenticity of product. The Compliance Officer should ensure that any new information regarding product authenticity indicators are documented and implemented. The purchase and sale agreement or purchase order should contain terms that govern should a vendor intentionally or unintentionally sell inauthentic product to the Member Company. These policies and procedures include notifying the manufacturer, quarantining product, and working with law enforcement. In keeping with the AscdiNatd Anti-Counterfeit Policy, in no event should inauthentic product be returned to a vendor. Any product not sent to law enforcement or the manufacturer for further investigation/prosecution should be destroyed. Member Companies should also notify the AscdiNatd office of any experience with counterfeit product and should submit photos and explanations of product deemed to be counterfeit to assist other resellers in identifying counterfeit. It should be the responsibility of the Compliance Officer to ensure proper recording systems are in place to track product from vendors.

F. EXPORT CONTROLS

The Bureau of Industry and Security ("BIS") is charged with ensuring effective export controls and compliance. BIS publishes guidelines that should be reviewed by the Compliance Officer if the Member

Company is involved in any international sales. Similar to these Best Practices, the guidelines include "Know Your Customer" (https://www.bis.doc.gov/index.php/compliance-a-training/export-management-a-compliance/freight-forwarder-guidance/23-compliance-a-training/47-know-your-customer-guidance) with a further link to "Red Flags" that is worth careful review. These documents are also available on the AscdiNatd website in the Legal Database, together with the Commerce Department's Introduction to Export Controls.

G. OEM PRACTICES

The Member Company's best practices guidelines for trading in new and used equipment and/or providing third party maintenance services to end users should address issues relating to the practices of the original equipment manufacturer ("OEM"). Whether or not there is any formal relationship between the Member Company and any OEM, the Member Company must be aware of the practices of the OEM's and the impact the intellectual property rights ("IPR") of the OEM can have on the Member Company's trading in OEM equipment.

1. Contractual Relationships

Where the Member Company has a formal relationship with an OEM (e.g., as a distributor, authorized or value-added reseller, financing partner, etc.), the relationship will be governed primarily by the contractual agreement in place between the parties. Unless the Member Company is a large company providing a significant business advantage to the OEM, the contract terms are likely to be dictated by the OEM. Nonetheless, the Member Company should ensure that there is full legal review of the agreements that are put in place in an effort to negotiate terms that are more favorable to the Member Company but at the very least, so that the Member Company and its Compliance Officer have a full understanding of the terms of the agreement(s) and the impact on day-to-day business practices at the Member Company. For example, a distribution agreement will likely limit the territory in which the Member Company may sell the OEM product. The Member Company should clarify how such limitations apply to customers who have multiple locations – can the Member Company sell wireless routers to all the Starbucks in its territory or can wireless routers only be sold to Starbucks corporate in Seattle? In another example, the Member Company may be allowed to access certain diagnostic software in providing third party maintenance. What are the limitations as to scope of access, duration, etc.?

2. Parallel Markets

Many Member Companies deal in new equipment that is sourced through a parallel market – sometimes called gray market. Parallel markets arise when new equipment is sold by the OEM or an authorized distributor of the OEM to a customer who then resells the new equipment into the open market. This may occur without the knowledge or agreement of the OEM or its distributor – i.e., the customer says it is purchasing the equipment for its own use but either has the intention from the start to resell the equipment; or later finds it has excess equipment and decides to resell the excess – or it may occur with the knowledge and agreement of the OEM or its distributor – i.e., the OEM or distributor wants to make the sale even though it realizes that the equipment will be resold by the customer. In either case, someone in that chain (even if it is the OEM's own Country Manager, for example) may be violating its agreement with the OEM's regarding reselling of the equipment. Member Companies should avoid purchasing from a source if that source has breached its agreement with the OEM.

OEM's often restrict the warranty offered with equipment. For example, equipment originally sold outside the U.S. is often not entitled to a U.S. warranty. Member Companies that are engaged in parallel markets need to be aware of such limitations and U.S. state or federal laws that govern parallel markets. For example, New York, Connecticut and California have "gray market laws" that require vendors to clearly publicize the fact if equipment being sold is not entitled to the manufacturer's warranty. While an equivalent warranty may provide a defense against such a restriction, the Compliance Officer should ensure that an appropriate disclaimer is included in the marketing of such equipment, particularly when the equipment is marketed on the Web and may be sold into jurisdictions with controlling gray market laws.

Some OEM's have challenged companies in the parallel markets directly by insinuating that the product being sold may not be new or may be stolen, and demanding that they clearly state that the manufacturer's warranty does not apply. Others have promulgated untested legal theories concerning "discount fraud", claiming that parallel market goods were somehow obtained fraudulently and demanding that the parallel market trader reveal information concerning the source of the equipment it is selling. While compliance with such demands and "requests" is likely not required, Member Companies and their Compliance Officers need to be aware of such practices and avoid exposure where possible. Finally, some OEM's make a conscious effort to confuse parallel markets with counterfeit goods. Parallel market goods are legitimate products that do not violate the IPR of the OEM and Member Companies and the AscdiNatd should emphasize the distinction to customers, CBP and other agencies.

3. OEM Software Issues

Challenges by OEM's concerning their IPR in software have impacted Member Companies in two particular areas. The first concerns the transfer of operating system (OS) software upon the resale of used equipment. This issue, often referred to as the right to transfer "imbedded software" is a priority for AscdiNatd in its legislative and lobbying efforts. Compliance Officers need to be aware of the terms of software licenses and ensure compliance. However, they should confirm with counsel whether OEM limitations are as represented. For example, an OEM sales rep recently warned a customer that transfer by a Member Company of its equipment with its OS violated license prohibitions against transfer of software. However, a more careful reading of the license provisions revealed an exception for "bundled software" – products that combine hardware and software where there is no separate product code or license fee for the software.

The second area of best practices regarding OEM software concerns accessing diagnostic or other maintenance software and patches in the course of providing hardware or software maintenance. The recent decision in Avaya v. Continuant would seem to provide a basis for maintenance companies to access maintenance related software, including software residing on OEM servers, in order to provide third party maintenance to legitimate customers and the decision even went so far as to find the OEM guilty of anti-trust violations for forcing customers to use Avaya maintenance services in order to receive the latest patches and fixes. Member Companies should be cautious in relying too heavily on the Avaya v. Continuant decision because other courts may not apply the same reasoning and the dust has not yet settled on the law coming out of that decision.
An ancillary effect of such activity is that Member Companies may be subpoenaed to provide documents or testimony in cases against others or under a regulatory proceeding. The cost of responding to such subpoenas can be significant, particularly due to the requirements of electronic data production. The Compliance Officer should establish a detailed document retention policy and should seek advice

concerning the storage of e-mails and other documents that will enable the Company to provide an efficient yet compliant response to such subpoenas. Such steps will also serve the Company well should the Company itself become the target of a lawsuit. Cases can be won or lost at the discovery stage and the ability to produce documents efficiently can significantly reduce the direct and indirect (diversion of Company resources) costs and provide a "leg up" in litigation.

H. TRAINING OF MEMBER COMPANY PERSONNEL

The Compliance Officer is responsible for implementing a program to train designated employees in connection with the Member Company's policies and procedures, the current law, and guidelines with respect to the Best Practices areas. The Compliance Officer should pay particular attention to:

- the necessity to be pro-active concerning the uncovering of illegal activities;
- the training of personnel to monitor for and detect counterfeit product;
- ensuring that product and OEM guidelines are updated on a regular basis from publicly available information;
- appreciation of the severity of regulatory and civil exposure due to lack of a pro-active stance;
- recognition of suspicious activity indicators and the procedures in place regarding vigilance when establishing a new relationship, and
- any other issues that the Compliance Officer believes would be educational.

The Compliance Officer should keep employees informed about relevant topics through presentations, through compliance alerts (copies of which should be maintained by the Compliance Officer), and through a Continuing Education Program. The Compliance Officer should ensure that written records (*e.g.*, agendas, memoranda, and notes) regarding these efforts are maintained, including (i) dates when such training was conducted, (ii) the nature of the training, (iii) the names of the staff who conducted and received the training.

I. INSURANCE AND DISASTER RECOVERY

The Compliance Officer should initiate a complete review of the Company's insurance coverage in light of its Best Practices guidelines. First, a careful review of property and casualty and business interruption insurance in light of increasing natural disasters is in order. Who would have expected that businesses in lower Manhattan needed flood insurance or that their businesses could be shut down for weeks while power was restored and damages repaired? For some, Superstorm Sandy was a death knell for their businesses due to lack of coverage. And it is surprising how many companies – even those involved in providing technology services – have no disaster recovery plan in place that can get them up and running in a new location with redundant technology services on short notice.

Next, Directors and Officers (D&O) and Errors and Omissions (E&O) coverage should be carefully reviewed with the issues covered in this paper in mind. The astronomical and unrelenting costs of litigation can severely undermine a Company's finances. Serious consideration should be given to spending more on insurance to provide coverage for the unexpected.

J. EMPLOYEE PRACTICES

The Compliance Officer should ensure that the Member Company has clearly described and communicated relevant Best Practices to its employees. Best Practices should be part of an Employee

Handbook which covers terms of employment, workplace behavior, benefits and all other employee-related matters. The promulgation of an Employee Handbook is a requirement in today's workplace and if the Member Company does not have one, the Compliance Officer should promptly initiate its development with the aid of counsel and HR advisors.

One of the issues to be covered with employees is that of gifts to customers or suppliers. Any gifts, rebates or donations must be commercially reasonable and within the guidelines established by the Member Company in consultation with outside counsel. The Compliance Officer should approve all gifts, rebates or donations and certify that they are within Company guidelines and reported pursuant to the current tax code(s).

K. INQUIRIES FROM LAW ENFORCEMENT AGENCIES.

Any inquiries from a law enforcement agency should immediately be referred to the Compliance Officer. The Compliance Officer, in consultation with counsel and Member Company principals, shall be responsible for answering any and all inquiries relating to customers/vendors or the Member Company's policies/procedures. The Compliance Officer, in consultation with counsel, shall be responsible for responding to all direct inquiries from federal and state law enforcement officers.

L. REVIEW OF THE COMPLIANCE PROGRAM

The Compliance Officer should be responsible for confirming that the Member Company's compliance program is reviewed on an at least an annual basis and that all deficiencies are addressed. In addition, the Compliance Officer should meet regularly with the Company's principals, attorney and outside accountants to review the compliance regime and consult on any outstanding matters. AscdiNatd will make an effort to provide updates and addenda to this Best Practices document. However, Member Companies should be aware that this document is meant as a guideline and that each Member Company should develop its own "Best Practices" to be understood by Officers, Directors and employees of the Company, no matter how large or small it is**.**

The Compliance Officer should also be responsible for ensuring that the documents used in the Member Company's transactions are up to date and address current legal issues. AscdiNatd provides forms of documents on its web site but the Compliance Officer should consult with counsel to be sure its specific issues are addressed.

Remember, the best protection your company has against the problems that arise in dealing in this complicated business environment is to put in place practices that pro-actively protect against such problems – in other words, Best Practices!