

NEVILLE PETERSON LLP

GLOBAL TRADE ALERT

Importer Identity Theft

July 2009

Identity Theft: A Growing Problem for Importers and the Trade Community

Customs Fraud Goes Virtual in the 21st Century

Your import manager gets a call from U.S. Customs and Border Protection. A shipment of footwear from China entered by your company has been seized at the Port of Los Angeles/Long Beach on suspicion of being counterfeit. A detention notice and property receipt are being issued, and you will receive a seizure notice shortly. In addition, you are advised, persons involved in trafficking counterfeit goods are subject to stiff monetary penalties under 19 U.S.C. §1526(f).

This could be a very serious problem. Counterfeiting is punishable by criminal as well as civil penalties. The owner of the trademark could sue your company for damages. And your company's reputation with Customs, not to mention its C-TPAT status, could be badly damaged.

Only one thing doesn't fit. You're an auto parts importer, not a footwear company.

What's going on?

Your Name. Your ID. But Not Your Stuff

The next day, you get the paperwork. That's your company's name and importer ID number on the entry documents. That's your customs surety bond code, and the shipping documents show the name of one of your Chinese suppliers. The invoice even describes one of the auto parts you import. If you get your Masterfile extract from Customs, the entry will show up as one of yours.

But other things don't fit. You don't recognize the Customhouse broker, the freight forwarder or the carrier listed on the documents. And the seized sneakers being held in Customs custody – phony as a \$3 bill – have no use in an auto, except maybe for covering the driver's foot as he pushes down on the gas pedal.

Welcome to the new world of Customs fraud. Your identity as an importer has been stolen, and used to import contraband. .

Importer Identity Theft: Surprisingly Easy

Hijacking the identity of a legitimate importer to enter contraband is remarkably easy. All that's really needed is the importer's Employer Identification Number (EIN) which is used as the importer number. Once a malefactor has your EIN, it's easy to forge a Customs power of attorney to hire a Customhouse broker to make entry. Once the bad guys know your company's name and EIN, other identifying details – address, names of corporate officers, lines of business – can usually be gotten quickly and quietly, from your firm's website, or from the Secretary of State in the State where you're incorporated (most of this information is also available online).

Customs' Automated Commercial System (ACS) makes identity theft easy. A Customs broker (who likely doesn't know that the power of attorney he's been given is phony) merely needs to enter your EIN into the ACS; the system will report back your address, Customs bond code and all the other information the broker needs to make entry.

And it's easy for the bad guys to make the phony transaction look real. There are a number of firms, such as Journal of Commerce/Piers, Zepol.com and others who publish import manifest data and make that data electronically searchable. While these companies provide valuable services to legitimate importers, the data they publish – like almost any other information in cyberspace – can be used to the wrong ends.

Suppose the bad guy wants to send counterfeit sneakers from Shenzhen, China to Long Beach Seaport. A quick search on one of these services might show that, for example, that "Acme Imports, North Hollywood, California", regularly imports at Long Beach air filters shipped by XYZ manufacturing in Shenzhen. So if the bad guy

generates some phony paperwork for the counterfeit sneakers, describing the goods as air filters shipped from XYZ in Shenzhen to Acme Imports in North Hollywood, it's going to look like a genuine and legitimate shipment in Customs' system.

Plus, the bad guys don't need to infiltrate the entire supply chain to pull these scams off. All they need is one willing participant in the U.S. – a forwarder, trucker, warehouseman – and the goods, once cleared by Customs, disappear into the stream of commerce.



Scams Galore: Here Are a Few

There are all sorts of identity theft scams being practiced on importers at present. Some, no doubt, have yet to be discovered. However, here are a few that our firm has seen repeatedly:

1. Identity Theft for Contraband Imports.

Recently, there were a number of cases in the Port of Los Angeles where parties trafficking in counterfeit Nike footwear made entry of that

footwear in the name of six (6) importers, whose identities were misappropriated. Customs detected the counterfeits and issued Notices of Seizure to the named importers of record, only to learn that the importers had no connection to the goods entered in their name. Still, the named importers needed to invest time and money to answer Customs and trademark owner inquiries, and avoid liability.

Because civil and criminal penalties for trafficking in counterfeit goods are so severe, it makes sense for the bad guys to piggyback on the names and reputations of legitimate importers.

2. Identity Theft for High-Risk Imports: Want to sneak in a shipment of goods that might be subject to 200% or 300% antidumping duties? Crooks have learned identity theft is the way to go. In recent years, we've seen an increasing number of cases where goods subject to substantial rates of antidumping or countervailing duties, such as shrimp, crawfish, mushrooms and furniture - have been falsely entered in the names of legitimate importers with no connection to the goods. In one recent case, a company whose business was importing cell phones needed to fight off a U.S. Court of International Trade lawsuit in which Customs was demanding \$2.5 million in antidumping duties and penalties owed on 4 entries of crawfish tailmeat. Modern cell phones have many features, but crawfish meat is not yet a popular (or available) cell phone app. The importer had to invest substantial sums to defend itself from the claims; its Customs bond surety may yet be tagged with the liability.

3. Know your Freight Forwarder. Recently, Customs seized shipments imported by three different companies, all of whom were represented by the same New York Customhouse broker. The broker had received all three accounts from a freight forwarder doing extensive business with Chinese shippers. The forwarder had transmitted to the broker Customs Powers of Attorney allegedly executed by the importers.

The Customs BRAVO (Broker Review and Verification Office) team in New York/Newark asked the broker to validate its retention by the three importers. When our firm examined the POAs, several irregularities emerged. The POAs were not signed by identified "officers" of the corporations; the contact phone numbers did not match the area codes for the companies' addresses; and a search to validate the names signed onto the POAs turned up the rather remarkable circumstance – probably not a coincidence – that all of the folks who executed the POAs had the same names as popular Ultimate Fighting Championship (UFC) competitors!

In these cases, Customs is looking to penalize the Customhouse broker for failing to exercise "responsible supervision and control" over the conduct of Customs business – even though the broker is as much a victim of the deception as anyone.

4. "Renting Out" Importer Identities A more recent development involves companies who have secured EIN numbers and Customs bonds and engaged Customhouse brokers, and who then decide to "rent out" their importer identity, for a fee. The broker will receive a request to enter merchandise in the importer's name – but once the merchandise clears Customs, the goods head elsewhere.

The goods may not be contraband, but the named importer of record, being neither the owner or purchaser of the goods concerned, does not have authority to make entry.

Typically, the importer identities are made available, for a fee, to Chinese shippers with no presence in the United States, and who do not want to bother qualifying as non-resident importers or posting bonds.

These scams are often carried out with the knowledge and cooperation of the named importer, but they represent a form of identity theft

nonetheless, since the importer's identity and bond are being misused. Customs could impose penalties not only on importers who allow their identities to be used this way, but also on Customs brokers for failing to verify that their principals had a legitimate connection to the goods being imported.

5. Filer Code Abuse A Southern California Customs broker recently had its three-digit "filer code" revoked by Customs, after the agency decided that the code was being abused, and used to make entries for firms having no connection with the imported goods. Customs now requires the broker to apply to Customs for an importer number before filing any entries – a crippling burden that threatens to put the broker out of business. The broker has sued, and its case is being litigated in the United States Court of International Trade on the question of whether a filer code is a protected property right and whether revoking a filer code is tantamount to revoking a Customs broker's license.

What Can Importers and Brokers do to Protect Themselves?

There are a number of common-sense steps which importers can take to protect themselves against the risks posed by identity theft.

1. Safeguard entry summary documents. Customs entries and entry summary documents (invoices, bills of lading, etc.) typically contain a lot of company confidential information – EIN numbers, supplier and carrier names, prices, etc. Importers should treat these documents as confidential, even after the transactions are over, and store them securely. An identity thief can learn a lot about your company just by reviewing an import entry.

2. Seek confidential treatment for inward manifest data. The Customs regulations contain a provision [19 C.F.R. §103.12] which allows importers to request that Customs treat as confidential, and withhold from publication, shipper and consignee/importer information appearing on inward vessel manifests. Customs will grant confidential treatment for two years at a time, subject to renewal. Importers should consider seeking such treatment.

3. Review available sources of data regarding your import shipments. Publishers such as Zepol.com provide a valuable subscription service for inward vessel manifest information. Companies should review their import transactions against these databases, to make sure they can identify all transactions being made in their name.

Also, Customs masterfile extracts and liquidation reports for your company should be reviewed periodically, to make sure you recognize all shipments attributed to you in CBP's system.

4. Monitor your Customs Powers of Attorney. Make sure you know who is authorized to file documents with Customs in your name. Make sure you know if a broker or forwarder issues a POA in your name to another broker. Revoke POAs to brokers you no longer use.

5. Loose Lips Sink Ships, And All That. Maybe your company has the highest clearance possible under the Customs-Trade Partnership Against Terrorism (C-TPAT). Maybe you've worked so closely with Customs that your import shipments are almost never inspected. You're deservedly proud. Good for you. But the whole world doesn't need to know it. If one of the bad guys thinks a shipment in your name is likely to sail through Customs, that makes your name a more attractive target for misappropriation.

Be careful about whom you share success stories with.

What Can Customs Do?

The fact is, Customs is running one of America's most important electronic commercial systems – the ACS – with very little in the way of identity security. As currently developed, the Automated Commercial Environment (ACE) is not much better, and being web-based, arguably even more subject to abuse.

Identity security is a matter which Congress and Customs will need to deal with. Here are two modest proposals to begin addressing the problem:

1. Establish a National Importer Registry.

Many countries have formal importer registries. If a company is not registered, and its bond or financial guarantee information supplied, it may not act as an importer of record. Moreover, importers are not approved until their information checks out.

Today, Customs has virtually no controls over importer identities. Any broker can electronically file a Customs Form 5106 importer identification form for a company and start importing in the company's name. Any broker with a company's EIN and access to ACS can start filing entries in that company's name. A national registry, which would not be invasive of privacy or confidential information, may be necessary.

Once importers are registered, Customs could begin supplying the importers with variable authentication codes, which the importers could supply to their authorized brokers, so that the brokers could make entry. The use of authentication codes would trip up identity thieves, and also prevent the filing of entries by brokers whose Powers of Attorney are "stale".

2. Electronic Issuance of Customs Powers of Attorney. Customs has no record of powers of attorney issued to Customs brokers. They grant access to ACS first, verify POAs later – after the damage has been done.

Most importers don't even know how many outstanding POAs they have issued, or have been issued in their name (i.e., by brokers to other brokers, by freight forwarders to brokers, etc.). Importers rarely formally revoke a POA when they switch brokers; even if they did, Customs has no way to know this.

Why not establish an online registration system for POAs? Customs would know who is authorized to represent particular importers, importers could have a verifiable record of POAs currently issued in their name, could revoke POAs electronically, and could identify possible phony POAs. Most brokers won't like disclosing client names, but if lobbyists can be required to identify their client names (and other details) as a condition of doing business with the Federal government, why not brokers?

It's a Group Effort

Fighting Customs cybercrime is a group effort. It requires the cooperation of import and logistics officials in the company, company counsel, internal corporate security, Customs brokers and other service providers.

In the past decade, importers have taken dramatic steps to professionalize their import procedures and techniques. Now it's important for importers to adopt security programs for the supply chain. The Customs-Trade Partnership Against Terrorism (C-TPAT) has taught thousands of companies to improve physical security during the movement of goods. It's time for companies to go the next step, and to harden their supply chains against cybercrime.

This means not only adopting information security procedures for Customs entries and other documents which contain sensitive information,

but also controlling the flow of information inside and outside the company. It means not only trying to legitimately limit the amount of data about your company's international trade operations that are published, but also taking advantage of sources of trade data as an important part of verifying the correct use of your company's identity.



Tighter control over Customs brokers, freight forwarders, carriers and supply chain partners is necessary for companies to make certain their identities are not misappropriated or misused. A good first start is a “scrub” – eliminating excess data, obsolete powers of attorney, and disposing of old entry and transaction data (subject, of course, to compliance with Customs' mandatory recordkeeping requirements).

Once the “scrub” is done, the importer should adopt and enforce internal and external information security policies, to make sure its identity is not misappropriated.

About Neville Peterson LLP

For over two decades, Neville Peterson LLP has been one of the United States' leading specialty law firms concentrating exclusively in international trade and Customs matters. With offices in New York City and Washington, D.C., and affiliated offices abroad, the firm has provided counseling and representation to clients before Customs authorities, administrative tribunals and courts around the world.

The firm also has extensive experience in antidumping, countervailing duty and trade relief proceedings, as well as a full-range export controls practice.

In recent years, Neville Peterson LLP has also represented clients on the forefront of international intellectual property issues.

The firm has an extensive litigation practice, and regularly appears before the United States Court of International Trade, the Court of Appeals for the Federal Circuit, Federal District Courts as well as foreign tribunals.

In recent years, the firm has presented seminars for many groups, including the American Association of Exporters and Importers; the Midwest Global Trade Association; the National Purchasing Managers Association; the Irish Exporters Association; the Mediterranean-American Business Network; and many others.

NEVILLE PETERSON LLP

17 State Street 1400 16th St., N.W.
New York, NY 10004 Washington DC 20036
212 635-2730 202 861-2959

www.npwtradelaw.com
