msk

did you do enough to protect your trade secrets?

MSK Client Alert

January 29, 2014

On January 21, 2014, Mozaffar Khazaee, a naturalized American who maintained dual citizenship with his native Iran, was indicted in Connecticut on two counts of interstate transportation of stolen property, which carries with it a potential sentence of ten (10) years in jail and a fine of up to $250,000. This case is a stark reminder that internal controls are only as good as their implementation.

What prompted the arrest was Khazaee's earlier attempt to ship 44 boxes of household goods to Iran. In fact, those boxes contained highly sensitive information about the U.S. Air Force's F-35 Joint Strike Fighter in the form of technical manuals, specification sheets, and other proprietary information. In order to stop Khazaee from leaving the country while the investigation is ongoing, a Homeland Security Investigation (HSI) agent swore out an affidavit to support an arrest warrant for violation of 18 U.S.C. § 234. The elements of the crime are 1) goods, wares, merchandise, or other property is stolen, converted, or taken by fraud; 2) the defendant transported, transmitted, or transferred the property in interstate or foreign commerce; 3) the defendant knew the property was stolen, converted or taken by fraud; and 4) the value of the property was $5,000 or more. The fact that the government relied on 18 U.S.C. § 234 as the basis to arrest him is worthy of comment since such a law clearly has nothing to do with the possible U.S. national security threat arising out of the attempted export.

The HSI affidavit explains that much of the contents of theshipment belonged to at least three (3) defense contractors. Press reports have identified one of the contractors as Pratt & Whitney, which has acknowledged it is cooperating with authorities. The affidavit makes clear these contractors all had in place exactly the types of agreement one would hope to find. Khazaee had signed a form of trade secrets agreement when hired in which he acknowledged he was responsible to surrender all company property upon termination. There were proprietary notices on many of the documents making clear the property belonged to the named defense contractor and was subject to the International Traffic in Arms Regulations or ITAR, 22 U.S.C. parts 120-130. There were also

attorneys

Susan Kohn Ross

practice areas

corporate & business transactions

intellectual property

international trade

notations on many pages that export contrary to U.S. law is prohibited. There was a general downsizing at Pratt & Whitney and, as part of his separation process, Khazaee signed an agreement stating he had returned all company property and complied with the company's intellectual property and business proprietary requirements. Yet he still had these reams of highly sensitive documents in his possession and was trying to get them to Iran!

Many have speculated why Iran would be interested in the information given the aging nature of its air force. The most likely reason is to assist its close allies, including the Chinese and the Russians. Perhaps Khazaee intended to go into business for himself. Whatever his motives, this case reminds companies of all sizes and in all industries that all the agreements in the world cannot protect you if they are not properly implemented and enforced. At this juncture, not enough is known publicly about how he obtained the documents. We do not know whether Khazaee emailed them to himself. Perhaps he had remote access and printed them. He could have also downloaded the files to thumb drives that he removed from the office. The HSI affidavit makes clear that some of the documents dealt with strength and durability evaluations for one contractor's engine components. Also in the boxes was a document entitled "Turbine Durability: Creep." Obviously these are highly sensitive business proprietary documents with potentially serious implications to U.S. national security.

Press reports indicate the F-35 program is centered around the concept of a single fighter plane designed to be used jointly by the Air Force, Navy, and Marines starting in 2015. As with any of these defense contracts, there are multiple parties involved, and a case like this one has to cause all of them to be concerned about how their information and technology is being handled.

One can find any number of reality shows featuring the dumb things criminals do. Certainly here, shipping anything directly to Iran would send up red flags, calling it household goods was even riskier, and trucking the boxes from Connecticut to Los Angeles for export to Iran generated even more red flags. Nonetheless, this case is a harsh reminder that monitoring what one's employees are doing can be tricky but remains necessary, especially if someone is being terminated.

Although we do not have details as to how Pratt & Whitney implemented its downsizing, this worst-case scenario serves to remind all employers that merely asking employees to sign confidentiality agreements is not enough to protect the confidentiality of company information – and this is an important factor whether, as here, we are focused on an employee no longer with the company or whether we focus on contractors or employees currently working with the company. Employers simply must take more measures to ensure that employees/contractors do not leave the premises with proprietary information, especially upon separation. These measures could include, for example, walking the employees/contractors back to their work stations and out of the building to ensure nothing is taken; ensuring that employees/contractors do not have access to computer systems at home (or, if they do have access, ensuring the IT department remains vigilant that nothing is downloaded without permission); marking all company documents as proprietary and confidential; having management remind employees/contractors regularly and consistently they must maintain company information confidential and that any violation of that policy will lead to discipline, up to and including termination; and filing charges or civil lawsuits against those employees/contractors who steal confidential information. Of course, these measures cannot offer complete protection against the enterprising malfeasant, but

they certainly send a message to other potential malfeasants the company will not tolerate the theft of its proprietary information.

los angeles
t 310.312.2000
f 310.312.3100

new york
t 212.509.3900
f 212.509.7239

washington, dc
t 202.355.7900
f 202.355.7899