

UNITED STATES DISTRICT COURT

for the
Southern District of Florida

United States of America
v.

Case No. 10-2098-White

Defendant

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

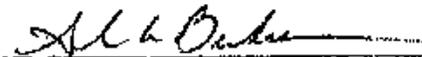
On or about the date of July 2007 to the present in the county of Miami Dade in the Southern District of Florida, the defendant violated 50 U. S. C. § 1705, an offense described as follows:

did knowingly and willfully export and attempt to export and cause to be exported U.S. made goods from the United States to the Islamic Republic of Iran by way of Hong Kong and Taiwan without having first obtained the required authorizations from the Office of Foreign Assets Control, in violation of Title 50, United States Code, Section 1705, and Title 31, Code of Federal Regulations, Section 560;

This criminal complaint is based on these facts:

See the Affidavit of Special Agent Alan Berkowitz

Continued on the attached sheet.



Complainant's signature

Alan Berkowitz, Special Agent, US Dept Commerce

Printed name and title

Sworn to before me and signed in my presence.

Date: 1-26-10



Judge's signature

City and state: Miami, Florida

Patrick A. White, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Special Agent Alan Berkowitz, U.S. Department of Commerce, Bureau of Industry and Security, ("BIS"), Office of Export Enforcement (hereinafter "OEE"), being first duly sworn, state as follows:

1. This affidavit is made in support of a Complaint and Arrest Warrant for YI-LAN CHEN, also known as "KEVIN CHEN" (herein referred to as "CHEN"). As set forth herein, there is probable cause to believe that CHEN violated and attempted to violate Title 50, United States Code, Sections 1701, *et seq.* ("the International Emergency Economic Powers Act" ("IEEPA")) and the United States Treasury Department's Office of Foreign Assets Control ("OFAC") comprehensive trade and investment embargo against Iran under the authority, *inter alia*, of IEEPA, as amended, Executive Order 13059 of August 19, 1997, which consolidates the provisions of Executive Orders 12613, 12957, and 12959, and the Iranian Transactions Regulations ("ITR") promulgated thereunder, principally, 31 C.F.R. § 560.204 ("the U.S.-Iran Embargo").

I. PERSONAL BACKGROUND

2. I am employed as an OEE Special Agent and have been so employed since August 1997. Before commencing my employment with OEE, I was employed as an Inspector with the United States Customs Service, now known as the Bureau of Customs and Border Protection ("CBP"), for approximately two years, and, prior to that, as a Revenue Officer with the Internal Revenue Service ("IRS") for approximately four years. Currently, I am empowered by law to investigate and make arrests for offenses involving, among other things, the unlawful export of goods and technology to destinations outside the United States.

3. As a Special Agent with OEE, I am familiar with and have received training regarding Federal laws relating to the unlawful export of goods and technology from the United States, as specified in the Export Administration Act of 1979 (hereinafter "EAA"), as amended (50 U.S.C. §§ 2401-2420), the Export Administration Regulations ("EAR") (15 C.F.R. §§ 736, *et seq*), and the IEEPA. I am also familiar with related federal laws and the interpretation and application of federal laws and federal court procedures, and I have previously conducted and assisted in the execution of numerous federal search and arrest warrants. I have conducted and participated in investigations of violations of United States laws relating to the unlawful export from the United States of goods and technology restricted for export for reasons of national security, foreign policy, anti-terrorism, and embargoed destinations.

4. I make this affidavit based upon my (a) personal observations and knowledge; (b) conversations with other law enforcement agents who have participated in this investigation and related investigations; and (c) review of documents connected with the investigation. Because this affidavit is being submitted for the limited purpose of establishing probable cause to obtain an arrest warrant/criminal complaint, I have not included details of every aspect of this investigation of which I am aware.

II. THE APPLICABLE LAW AND REGULATIONS

5. The President of the United States, by virtue of the IEEPA, is granted authority to deal with unusual and extraordinary threats to the national security and foreign policy of the United States. On March 15, 1995, the President of the United States, following previously issued Executive Orders, continued to declare a national emergency with respect to the Islamic Republic of Iran, finding the policies and actions of Iran constitute

a threat to the national security of the United States due to Iran's support of international terrorism and its attempts to acquire weapons of mass destruction.

6. On May 6, 1995, the President declared a trade embargo against Iran and prohibited the exportation from the United States to Iran of any goods, technology, or services, with limited exceptions for publications, other informational material, and donated articles, such as medical supplies intended to relieve human suffering. Prior to May 6, 1995, the export of any good or technology required approval of and the issuance of a license by the Department of Commerce. On August 17, 1997, the President reiterated and renewed the U.S.-Iran Embargo, which continued throughout the time of the events of this affidavit.

7. To implement the U.S.-Iran Embargo, the United States Department of Treasury through the Office of Foreign Assets Control ("OFAC"), issued the ITR (31 C.F.R. §§ 560.203-560.205) in September 1995. These regulations prohibit the export of goods from the United States to Iran unless authorized by the Department of Treasury. (31 C.F.R. § 560.204). The regulations further prohibit any transactions evading or avoiding the Iran Embargo, including the exportation of goods from the United States to a third country if the goods are intended for or destined to Iran. (31 C.F.R. § 560.203). Violation of the U.S.-Iran Embargo and the ITR is a federal felony offense punishable by up to twenty years' imprisonment. See 50 U.S.C. § 1705(a) and 31 C.F.R. § 560.204.

8. The Department of Commerce also has the authority to regulate the exportation of goods and technology from the United States to foreign countries. The Department of Commerce has issued the EAR, controlling the export of goods and technology to Iran. Under both the Department of Treasury and the Department of Commerce regulations, any individual must file an application for a license and receive approval

from the OFAC and/or Department of Commerce to export or attempt to export any goods or technology from the United States to Iran.¹

9. Both the Department of the Treasury and the Department of Commerce regulations are designed to control exports of United States commodities by prohibiting the export of goods which may have a detrimental effect on our national security. These regulations and controls focus both on the nature of the goods to be exported and on the end use and end user of the goods. Therefore, the regulations may prohibit exports and require licenses and authorizations from the appropriate agencies based on either the end use or end user of the goods or on the nature of the goods themselves.

III. PROBABLE CAUSE
A. BACKGROUND OF THE INVESTIGATION
INTO THE IRANIAN PROCUREMENT NETWORKS
AND THE USE OF EMAIL COMMUNICATIONS
IN FURTHERANCE OF ILLEGAL EXPORTS FROM THE UNITED STATES

10. OEE investigators, including your affiant, in the Miami Field Office are conducting ongoing investigations into numerous networks of individuals and entities in Iran that are engaged in the business of illegally procuring U.S. manufactured commodities for customers and end-users in Iran. These investigations have revealed that these Iranian procurement networks use suppliers located throughout the world, including suppliers in the United States, to obtain the U.S. commodities and that they use trans-shipment points throughout the world to attempt to circumvent the prohibition against exports from the U.S. to Iran. The trans-shipment points throughout the world are mid-way points

¹ As is apparent for the below-described illegal transactions and activities involving CHEN, CHEN acted as part of an illegal conspiracy to violate United State export laws and defraud the United States. It is a violation of the IEEPA to conspire to violate the U.S.-Iran Embargo and the ITR (50 U.S.C. § 1705(a)), and conspiracy to defraud the United States is also illegal (18 U.S.C. § 371). However, this affidavit is intended only to set forth the bases upon which there is probable cause to arrest CHEN and, therefore, it does not contain an exhaustive recitation or list of all of the laws CHEN is alleged to have violated nor all of the illegal acts in which CHEN is alleged to have been involved.

used by Iranians to do business with United States businesses as a means to deceive the United States businesses, who are led to believe that they are not doing business with prohibited destinations. The investigations have also revealed that the networks of individuals and entities engaged in the illegal procurement of goods often use email accounts hosted by U.S. based internet service providers ("ISPs") and internet hosting providers ("IHPs") in furtherance of their illegal procurement activities. Thus, a large part of OEE's ongoing investigation of illegal Iranian procurement networks has focused on email communications regarding the illegal exports, attempted exports, and shipments of U.S. commodities to Iran.

11. The individual who is the subject of this affidavit is known to investigators as YI-LAN CHEN and is also known to use the alias "KEVIN CHEN." As set forth below, investigators know that that CHEN uses two U.S. hosted email accounts, herein referred to as *Email Account 1* and *Email Account 2*, to do business with the United States and to supply U.S. commodities to individuals and entities in Iran, in violation of the IEEPA, the U.S.-Iran Trade Embargo, the ITR, and the EAR.

**B. CHEN'S PROCUREMENT AND ATTEMPTED PROCUREMENT
OF U.S. COMMODITIES FOR IRANIAN CUSTOMERS**

12. As detailed below, CHEN facilitated the shipment of numerous U.S. origin goods from the United States to Iran by way of Hong Kong. The below detailed transactions are not an exhaustive list of the shipments facilitated by CHEN for his Iranian customers. Rather, investigators have reviewed evidence reflecting that from early 2007 to the present, CHEN has facilitated the export of more than 30 shipments of U.S. commodities from the United States to Iran in violation of United States export laws. All of those shipments involve misleading United States businesses and United States

export enforcement agencies, and nearly all of those shipments involve dual use goods,² like those described below.

1. Attempts to Procure EFI Detonators

13. As part of the above-described ongoing investigation, numerous search warrants for the contents of email accounts used in furtherance of the above-described illegal procurement activities have been authorized by United States Magistrate Judges in the Southern District of Florida and executed by investigating agents. While reviewing email communications seized from the searched accounts, investigators discovered attempts by individuals in Iran to procure 2500 EFI Detonators. These individuals in Iran sent requests for quotes ("RFQ"s) to individuals in the United States in an effort to procure the detonators.

14. On July 28, 2008, OEE Special Agents met with representatives of a California company. During this meeting, Agents inquired if the California company had completed any sales of the aforementioned items. The company representatives responded that although they had not completed sales matching the specified RFQs, they had recently received a suspicious RFQ for 2000 of the same Detonators, along with the associated test kit and bridge cables. The request was sent to them by an individual identifying himself as KEVIN CHEN and using *Email Account 1*.

15. Records obtained from the U.S.-based internet hosting provider ("IHP") for CHEN's email accounts indicate that *Email Account 1* was opened with the IHP on March 09, 2007, from an internet protocol ("IP") Address originating in Taiwan. The

² Certain goods and technologies that have commercial application, but also could make a significant contribution to the military or nuclear potential of other nations and could be detrimental to the foreign policy or national security of the United States are commonly referred to as "dual-use" goods and technologies.

owner of the account is listed as KEVIN CHEN, and a secondary Taiwan-based email address is listed as the only contact information for the account. Nearly all access to this account has been from IP³ addresses originating in Taiwan.

16. According to company representatives, CHEN's responses to routine questions regarding the intended use of the detonators and the end-user raised suspicions about the order. Follow-up investigation by investigating agents regarding the information provided by CHEN confirmed that CHEN's information was misleading, inconsistent, and suspicious.

17. The detonators that were the subject of the above requests are controlled for export for national security reasons due to the fact that they have various potentially dangerous applications (including applications in missiles, explosives, and weapons technologies). Therefore, any export of the detonators would require that the purchaser/exporter obtain a license from the Department of Commerce prior to export. To date, neither CHEN nor Landstar Tech has applied for or received a license to export such detonators. Moreover, if, as investigating agents suspect, CHEN intended to export the detonators for eventual export to Iran, the transaction would require additional licenses from OFAC. To date, neither CHEN nor Landstar Tech has applied to OFAC for the export of the detonators (or any other item) to Iran.

18. According to representatives of the California company, communications with CHEN broke off soon after CHEN responded to initial requests for end-user information. No sale of the detonators was made to CHEN, and he has not contacted the company since approximately July of 2008. However, as a result of the information learned from

³ An Internet Protocol (IP) address is a unique numeric identifier assigned to every computer attached to the Internet. An ISP normally controls a range of several hundred (or even thousands of) IP addresses, which it assigns to its customers for their use.

the interview of the California company representatives about CHEN's efforts to procure the detonators, OEE initiated an investigation into CHEN's export activities.

19. During the course of the investigation, between February 2009 and December 2009, United States Magistrate Judges in the Southern District of Florida issued search warrants and court orders for searches of CHEN's U.S.-based email accounts.

2. Procurement of P200 Turbine Engines

20. In the course of analyzing information obtained during searches of CHEN's email accounts, investigators discovered that on July 31, 2007, CHEN received an email request to his *Email Account 1* from an individual in Iran. This email was sent using an IP address registered in Iran. In it, the sender requests a quote for six U.S. manufactured P200 Turbines plus 150 sets of spare parts. According to the U.S. manufacturer, these engines and spare parts are model airplane turbine engines and spare parts, but they can also be used to operate unmanned aerial vehicles. In fact, the U.S. manufacturer advised investigators that they do sell these engines for military use in target drones.

21. On August 20, 2007, CHEN sent an email from his *Email Account 1* to the U.S. manufacturer in California and placed an order for two sets of P200 engines and spare parts. In that email, CHEN requests that the seller bill his company, In-Tech Company Ltd (a Taiwanese company identified as belonging to CHEN), and ship the items to a Hong Kong freight forwarder, Acteam Logistics, Ltd.

22. On August 31, 2007, CHEN sent an email from his *Email Account 1* to Acteam regarding the P200 starter shipment. In it, CHEN informs the freight forwarder that three boxes would be arriving from the U.S. via UPS to their Hong Kong office on about September 5th or 6th; that he would have his Iran customer arrange pick up via DHL; and

that the customer in Iran would pay DHL costs from Hong Kong to Iran. CHEN also attached a copy of the commercial invoice value for the Hong Kong to Iran shipment. The attached In-Tech Company, Ltd commercial invoice names the Iranian purchaser and lists a Tehran, Iran, address for the purchaser. In the commercial invoice, CHEN lists the items as a starter for a car and wheels.

23. On September 7, 2007, the two P200 Turbines and spare parts were shipped from California to Acteam Logistics Ltd. in Hong Kong via UPS. On September 13, 2007, CHEN informed the sales representative via email that he had received the UPS shipment and requested 150 pairs ceramic bearings for the P200s. On November 12, 2007, four R7009 Bearings for the P200s were sent from California to CHEN/Acteam in Hong Kong via UPS. On October 23, 2007, CHEN sent an email to his Iranian customer informing him that the bearings had been sent to the Iranian customer via DHL.

24. According to Department of Commerce, BIS license determination number G076618, dated November 24, 2009, the P200 turbine engines and spare parts are classified under Export Control Classification Number (ECCN) 9A991.d, for Anti-Terrorism reasons, and would require a license or authorization from OFAC prior to export. No license or authorization was obtained in this case. Export of these engines to Iran without a license or authorization from OFAC is a violation of the IEEPA, the U.S.-Iran Embargo, and the ITR.

3. Procurement of Sealing Compound

25. Investigators also discovered that in April 2008 CHEN was involved in another procurement of U.S. commodities for Iran after he inserted himself into an ongoing

transaction for the same Iranian customer as involved in the P200 Engine shipments with an on-line chemical distributor for the purchase of nine quarts of MIL-S-8516 sealing compound. Sealing compound (MIL-S-8516) is an accelerated, synthetic, rubber sealing compound used for sealing low-voltage electrical connectors, wiring, and other electrical equipment against moisture and corrosion where temperatures do not exceed 200°F. This particular sealant is designed to military specifications ("MIL-S") and is manufactured in Pacoima, California. The sealant has numerous applications in military, aerospace, and automotive industries. It is considered a hazardous material for shipping purposes.

26. On April 9, 2008 CHEN sent an email from his *Email Account 1* to a sales representative for the California distributor of the sealing compound. In that email, CHEN informs the sales representative that he (CHEN) would be handling the sale and shipping of the sealing compound due to the "Dangerous Cargo" designation of the sealing compound.

27. Later, on approximately April 10, 2008, CHEN sent an email to Acteam Logistics in Hong Kong requesting a quote for the cost of shipping dangerous goods from Hong Kong to Iran. To that email, CHEN attached the product description for 9 quarts of MIL-S-8516 sealing compound. Then, on April 12, 2008, CHEN sent an email to his Iranian customer in which he requests a wire transfer of US \$4,500 ~ \$5,000 to a Landstar Tech Company Ltd bank account for the purchase of the sealing compound. On April 16, 2008, CHEN sent his Iranian customer an email with a copy of the pro forma invoice for the sale to the Iranian customer of 9 quarts of sealing compound, item #MIL-S-8516, which indicates shipment to Tehran and requests authorization to place the order. Later, on April 16, 2009, the Iranian customer replied via email and directed CHEN to

place the order. Then, on April 20, 2008, CHEN confirmed the sealing compound order via email to the California company's sales representative and informed the sales representative that (US) \$1,862.50 would be wire transferred on that date. CHEN also provided a shipping address as Acteam Logistics Ltd., Hong Kong.

28. On May 14, 2008, the Iranian customer sent CHEN an email instructing CHEN to change the consignee name and address for the sealing compound shipment to a different recipient with an address Tehran, Iran. Investigative research reveals that listed consignee address is linked to Electro SANAM Industries. According to www.iranwatch.org, part of the Wisconsin Project on Nuclear Arms Control, Electro SANAM Industries is a known front company for Aerospace Industries Organization ("AIO"), Iran and has been linked to Iranian ballistic missile programs. AIO conducts research and development on ballistic missiles and is a leading industrial and military subsidiary of the Ministry of Defense and the Ministry of the Armed Forces Logistics of Iran (Ref.: Report J 207, May 2009.) Electro SANAM Company (aka E. S. Co., E. X. Co.) is listed in annex IV of U.N Security Council Resolution 1803 dated March 3, 2008 for links to nuclear proliferation activities.⁴

29. On May 14, 2008, CHEN received an email from the sales representative with a copy of a shipping company air waybill, showing the export of the sealing compound from Los Angeles, California, to Hong Kong on May 14, 2008. Subsequently, on May 22, 2008, CHEN received an email from his freight forwarder in Hong Kong, Acteam, informing CHEN that the sealing compound was scheduled to ship to Iran on May 23, 2008, and providing the air waybill number and flight information. CHEN, in turn, sent an email to his Iranian customer informing him that the items would be arriving in

⁴ *Iran Watch*, 8/27/2008, Website [<http://www.iranwatch.org/suspect/records/electro-sanam-company.htm>]

Tehran in two days and listing the air waybill number and flight number previously provided by CHEN's freight forwarder.

30. The export of the sealing compound MIL-S-8516 to Iran without OFAC authorization is a violation of the US-Iran Embargo and the IEEPA. No license or authorization was obtained for this shipment.

4. Procurement of Glass to Metal Seals

31. On July 13, 2008, CHEN, using his *Email Account 1*, sent an RFQ to a New Bedford, Massachusetts, company and its related New Jersey company, seeking 5,000 glass to metal pin seals. Glass to metal pin seals are commonly used to hermetically seal a conductor pin in a metal feed thru in an electrical device. These have many applications, such as vacuum components, sensor or transducer housings, feedthroughs for harsh environments, and battery headers. The nickel alloy specified in this Landstar Tech order was DIN 2.4478, otherwise known as "Alloy 52." This alloy is commonly used in semiconductor applications. In fact, CHEN's Iranian customer for the pin seals provided a drawing from its ultimate customer in Iran which depicts a custom engineered terminal assembly using a specific glass-to-metal seal. Investigative research reveals that the design and engineering of the depicted seal makes it ideal for exposure to high pressure, vibration, and extreme temperatures. The possible applications of an assembly with this level of consideration to high performance materials could include aerospace, thermal imaging devices, chemical agent monitors, and weapons systems.

32. When asked by the supplier for an End-User Statement regarding the purchase of the seals, CHEN provided a document indicating that Landstar Tech Co. in Taiwan was purchasing the seals but that the ultimate end-user was Tex-Co Ltd, in Hong Kong.

This statement is not only false and misleading, but it raised a red flag for investigators who know that Tex-Co Ltd is a freight forwarder. In fact, Tex-Co Ltd was listed by CHEN as the freight forwarder when negotiating the purchase of the above-discussed detonators allegedly destined for the Taiwan Welding Precision Company. Freight forwarders are not proper end-user designations. Rather, a proper end-use statement must indicate the ultimate destination of the goods rather than a transshipment point. In November 2008, the New Jersey company shipped 5,000 glass to metal seals to Tex-Co Ltd in Hong Kong.

33. Evidence obtained during the search of CHEN's *Email Account 1* includes documents showing that the glass to metal seals shipped from New Jersey to Tex-Co Ltd in November 2008 were forwarded by CHEN to the customer in Tehran, Iran. Investigators also found Landstar Tech's October 2008 Pro-forma Invoice and November 2008 Commercial Invoice issued to the customer in Tehran, Iran. Additional documents recovered from CHEN's *Email Account 1* show that on February 4, 2009, the New Jersey company shipped an additional 5,000 pieces of the glass to metal seals to Tex-Co Ltd, who were instructed in emails from CHEN to send them on to Iran.

34. The export of the glass to metal seals to Iran without OFAC license or authorization is a violation of the IEEPA, the U.S.–Iran Embargo, and the ITR. No license or authorization was obtained for this shipment.

5. Attempts to Procure Connectors

35. Further analysis of the data obtained from searches of CHEN's email accounts revealed that CHEN has another Iranian based customer. This other Iranian customer is the owner of the Noavaran Sooyab Sanat Co. in Tehran, Iran. Sooyabsanat Co. was founded in 1989 as an Instrumentation division of Jahad Engineering Research Center.

Jahad Engineering Research Center is one of many names used by the Engineering Research Center for the Construction Crusade (Jihad-e Sazandegi) located in Tehran, Iran, which has been linked to chemical research and development facilities. According to www.iranwatch.org, part of the Wisconsin Project on Nuclear Arms Control, in 2006, Jahad Engineering Research Center has been listed as an entity of concern by the British government for Weapons of Mass Destruction related procurement concerns.

36. On August 8, 2009, CHEN received an email RFQ from an individual identifying himself as "Ali", from Sooyabsanat, for 60 pieces of "connectors". That email, in pertinent part, follows:

Subject: Again Ali from Sooyab...
From: sooyab engineering <[]>
Reply To: [] Date: 8/8/2009 8:37am
To: [Email Account 1]

Hello dear Friend Kevin,

How are you? I hope best wishes for you. You know we need some connectors that I have attached photos of it for about 60 pieces. Its order code is MS3132H7Y50P. We need male part.

You know, Iran is under sanction! So would you please contact following address to see if they have such connector in stock and what about price?

The specified connectors, Circular Hermetic Connector, Model MIL-C-81703, are designed to facilitate the flow of electrical current across two devices and can be mechanically coupled to, or uncoupled from, another connection. The connectors are designed to military specifications ("MIL" Spec) and have aerospace, defense, industrial, and petrochemical applications. For example, they may be used to provide connectivity between instrument displays and the computer hardware that controls them.

37. After receipt of the above RFQ, CHEN communicated back and forth with Sooyabsanat and the U.S. supplier, and eventually responded back to his Iranian customer on August 22, 2009. This August 22, 2009, email makes it very clear that CHEN is aware that he is violating U.S. export laws by shipping U.S. goods to his Iranian customers:

Subject: Fwd:Again All from Sooyab...
From: Kevin Chen [Email Account 1]
Date: Sat, 22 Aug 2009 11:34:17 +0800
To: "[]" []

Dear [],
Regarding the [] connector, we have got the shipping cost from [] company, USA to Hong Kong. We also asked them to send us Specification sheets for your approval. By the way, we have also issued the P/I to you as per attached file. If everything is ok, we will be waiting for your total payment of US\$5,300 to confirm this order.

As you know we can not tell USA this connector is for you. So we have to tell a white lie to USA that this is for our factory in Hong Kong, so USA will ship to our office in Hong Kong. We will ship these 60 pcs of connector to you from Hong Kong by ARAMEX. So please kindly arrange the US\$5,300 to the below bank account:

The Hongkong and Shanghai banking Corporation Ltd
1 Queens's road, central, Hong Kong
Swift code: []
Account no. []
Beneficiary's Name: Landstar Tech Company Ltd

Best regards
Kevin.

38. On November 3, 2009, CHEN sent an email from *Email Account 1* to the Iranian customer in which CHEN asks the Iranian customer to advise how much CHEN should indicate as the value of the invoice for purposes of shipping the 60 pieces of connectors from Hong Kong to Tehran by Aramex. Based on my experience and that of other agents working on this and similar investigations of Iranian procurement networks, I know that shippers often undervalue items on paperwork accompanying shipments into

Iran for the purpose of avoiding excessive import tariffs in Iran and also to avoid the detection of both domestic and foreign law enforcement.

The Iranian customer responded as follows:

Subject: re: Invoice values of 2 shipments
From: "[]"
Date: Tue, 3 Nov 2009 01:12:20-0500
To: "Kevin Chen" <[Email Account 1]>

Dear Kevin
1-[] connector with 5 USD is ok.
2-8460 Y36 magnet, 0.25 USD is ok.
Best Regards
[]

Subject: Invoice values of 2 shipments

From: Kevin Chen [Email Account 1]
Date: Tue, 3 Nov 2009 10:12:55 +0800
To: [] []

Dear [],
1) 60 pcs of [] connector (from Hong Kong to Tehran by ARAMEX)
Please advise how much invoice value you want me to make for these 60 pcs??

2) 8,460 pcs of Magnet Yoke (from Taiwan to Bandar Abbas by sea)
Please advise how much invoice value you want me to make for these 60 pcs??

Best regards
Kevin

a. Seizure of the Electrical Connectors Shipment

39. In November 2009, OEE agents intercepted the shipment of the 60 electrical connectors en route to CHEN from the United States. On November 4, 2009, this affiant sent CHEN an email from my official BIS email account and requested that CHEN provide end-user information for this shipment by filling out BIS Form 711. On November 5, 2009, CHEN sent this affiant a response by email from his *Email Account 1* and attached a completed BIS Form 711. On the form, CHEN lists the end user of the items as Tex-Co Ltd. in Hong Kong and states the items will be used in manufacturing

and will not be re-exported from Hong Kong. As discussed above, Tex-Co is one of CHEN's freight forwarders in Hong Kong which CHEN uses to send items to Iran.

40. On November 23, 2009, CHEN sent this affiant an email from his *Email Account 1* to my official BIS email account asking for my assistance in filling out the BIS form 711 in order to get the 60 pcs of connectors released. In that email, CHEN states that the connectors will be used to repair the hydraulic valves of the air conditioner of a subway system. This is a different end use than the one he originally stated on the BIS Form 711 he supplied on November 5, 2009. CHEN also requests that I call him to discuss the matter.

41. Shortly after reading this email, on November 23, 2009, this affiant placed a monitored and recorded telephone call from my BIS Miami Field Office to CHEN and informed CHEN that the end use information provided by him and Tex-Co in Hong Kong for the shipment of the 60 electrical connectors was not sufficient. This affiant advised CHEN that we have information that Tex-Co is a freight forwarder and not a proper end user and that Tex-Co had indicated that the connectors were for use on a production line, which is different from CHEN's claim that the items are to be used to repair hydraulic valves on the air conditioner of a subway system. This affiant further advised CHEN that in order for the parts to be released, CHEN needs to provide specific, detailed information from the subway end user, including where and what subway, who operates the subway, a point of contact at the subway, and documentation regarding his contract with the subway. CHEN asked your affiant what will happen to the shipment if CHEN cannot provide the requested documentation, to which your affiant advised CHEN the items would not be sent to him and could end up in a government warehouse indefinitely. To date, there has been no further contact from CHEN to your affiant.

However, CHEN has continued to reach out to representatives from the supplier, seeking additional shipments of products and requesting assistance with the seized shipment.

b. Introduction of Undercover Agent

42. On December 11, 2009, an OEE Agent acting in an undercover capacity ("U/C") as an employee of the U.S. supplier of the electrical connectors began a series of email communications with CHEN at CHEN's *Email Account 1*. In a December 11, 2009, email, the U/C engaged CHEN by informing him that he believes that the items detained by the U.S. Government are not going to be released. The U/C also told CHEN that he (the U/C) believes that CHEN's business, Landstar Tech in Taiwan, and the freight forwarder in Hong Kong may be flagged by the U.S. Government. In the same email, the U/C asks CHEN: "Do you have any other options or suggestions as to how I can get the parts to you." The U/C also tells CHEN, "I am looking for suggestions from you as to how I can continue to serve your needs without either one of us getting into trouble."

43. On December 11, 2009, CHEN replied to the U/C email and stated that he agrees that the items will not be released by Customs. CHEN then inquires if the U/C is able to get CHEN an additional 60 pieces of the connectors and ship them to an address other than the freight forwarder in Hong Kong, suggesting that the U/C send the connectors to Landstar Tech.

44. On December 14, 2009, the U/C responded to CHEN as follows:

[U/C] [] Mon, Dec 14, 2009 at 1:47 PM

To: Kevin Chen [*Email Account 1*]

Dear Kevin,

I'm glad that you have agreed to handle the matter in this way. I also appreciate that you have placed your trust in me to get you the items that you and your customers require. I am concerned that even Landstar will be flagged. I have seen this sort of thing happen before. Once US

Customs detain a shipment, they start asking questions. If you dont have the answers that they want/need, they will then start looking deeper into what you are doing. Listen, I do not want you to take that chance. I want to help. Here is what I propose.

I want to let you know that I do work outside of [my employer]. I have experience in getting around US Regulations and Customs. For instance, I have been able to supply everything from basic consumer electronics to bigger ticket items like military aircraft parts. Put it this way, my income suffers if I can't get something for my customer. Therefore, I can get you anything you and your customers need, regardless of where they are located. I have, for many years been able to get shipments to my customers who are located in countries that the US prohibits from doing business with. I have been extremely successful in doing this. Plus, with your help, I may be able to establish a reliable "friend" in Taiwan to assist me with my future needs of getting things into the middle east. Dubai used to be a great place for this purpose, however things are getting to hot there right now. I need to start looking for other places to tranship the goods.

Therefore, I suggest that you provide me with someone else that you can trust. Use another company to purchase the items from me, use their letterhead for quotes, purchase invoices, ect. I will process it as a new customer and ship the items to that location. You may have to pay a small fee to the other business, unless they are your friend, but you simply pass those costs onto your ultimate customer saying that [my employer] has raised their rates. I, in turn, will provide you with a "real" invoice" and a fake invoice so that you can provide to your customer which reflects the higher price. Hell, you might even make more money for yourself by doing it this way. If you agree to this, please check the following for what I can do for you.

* * *

Please let me know what you think. Also, keep in mind that I can get you military parts and other things that [my employer] does not sell.

Looking forward to a long and prosperous relationship.

[U/C]

45. CHEN replied via email to the U/C that same day, December 14, 2009. In that email, CHEN states: "I am very glad to know that you are so flexible to do the business. This is very helpful for us." CHEN also writes: "We are not going to do BIGGER tickets ...because this is not our aims. What we want is to do the business by means of safe and low profile then nobody gets hurt." CHEN goes on to inquire whether the U/C is able to ship the items to the U.S. supplier's Shanghai office and whether the U/C has "a reliable friend who can help this situation." After discussing details regarding terms and conditions for future shipments of the connectors, CHEN writes: "You remind me that you can do other business that [your employer] doesn't sell. This is a good news. I

would like to know how you are handling it. For example, if we want to buy a product (suppose it is not military things nor sensitive things), how to do business with you? Do you have friend who is doing this? or you do it your own private company? I am very interested to know it because we may have business chance on it."

46. On December 17, 2009, the U/C sent an email to CHEN stating he (the U/C) was unable to send the items to Shanghai. In that email, the U/C goes on to suggest a possible meeting in person in CHEN's region of the world in order to discuss future business possibilities. The U/C also suggests that he (the U/C) may be able to bring the 60 pieces of connectors that CHEN is still trying to get from the U.S. to CHEN at this meeting. To this, CHEN responded on the same date, December 17, 2009, as follows (in pertinent part):

Kevin Chen [Email Account 1] Thu, Dec 17, 2009 at 8:38 PM
To: [U/C] []

Dear [U/C],

...
I really like your idea of meeting each other in our area. (Hong Kong or Taiwan will be fine with me) Actually this is the BEST way of getting these parts. It solves 2 problems in one time (payment & shipment). Please let me know if we should start now? If I just place 2nd order to you with 20% discount via Landstar company? I prefer this way because there is no other company I can think of helping us about this order.

About your fee, I can always hand over to you when we meet each other. This is definitely no question about it.

Regarding future business, I am very very sure we can do something and we both can enjoy the business for long time. We really have to meet each other and discuss our plans for future business. Regarding those items you mentioned, frankly speaking I don't do that BIG items & sensitive items because this is too risky and this is not my main business. Anyway, we can discuss when we meet each other. (remember we have 2 orders in [your colleague]'s hands now and one more is coming soon. So we have good chance to cooperate)

Are you coming to Asia often? When you will come next time? I am very looking forwarder to seeing you soon and we can talk about our partnership face to face.

Have a nice day!

Best regards
Kevin

47. On January 4, 2010, the U/C sent an email to CHEN and advises that his business partner is unable to meet in Hong Kong and suggests they meet in Saipan, Mariana Islands, in early February. CHEN responded the following day that he cannot travel to Saipan and encourages the U/C to travel to Hong Kong to meet with CHEN and to complete the delivery of the connectors prior to the Chinese New Year (mid-February).

48. On January 7, 2010, CHEN sent an email to the U/C suggesting that they meet in Guam. To this, the U/C responded via email on January 8, 2010, confirming that he and his business associates are able to meet in Guam and that the U/C will bring with him all of the orders that CHEN has outstanding with the U.S. supplier. On January 11, 2010, CHEN sent an email to the U/C confirming that CHEN will be arriving in Guam on February 3, 2010, and will be staying three nights. CHEN also asks for confirmation from the U/C that he will be hand-carrying all of CHEN's outstanding orders for him.

49. According to BIS Certified License Determination number G076755, the Circular Hermetic Connector, Model MIL-C-81703, which is part number MS3132H7Y50P, is classified under Export Control Classification Number EAR99 and requires Department of Commerce and/or OFAC authorization to be exported or reexported to Iran. Neither CHEN nor Landstar Tech has applied to the Department of Commerce and/or OFAC for authorization to export the connectors to Iran and, therefore, the export of the connectors would be a violation of the IEEPA, the U.S.-Iran Embargo, the ITR, and the EAR.

IV. CONCLUSION

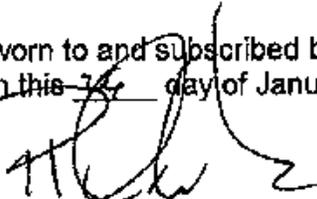
50. Based on my training and experience as an OEE Special Agent, I know that individuals engaged in illegal export activities often provide false information regarding

the ultimate destination of goods in order to deceive U.S. businesses and export enforcement authorities and to conceal the fact that the goods are going to a prohibited destination or that they require a license for export. I also know that purchasers in prohibited destinations, like Iran, often use intermediary destinations for transshipment of goods from the U.S. as part of their efforts to circumvent export restrictions. Based upon the evidence seized during searches of CHEN's email accounts, investigators know that CHEN has been doing business with the United States and, as such, in the United States, and has orchestrated the shipment and trans-shipment of numerous U.S. goods to Iran by intentionally deceiving U.S. businesses and U.S. export enforcement authorities, in violation of the IEEPA, the U.S. - Iran Embargo, the ITR, and the EAR.

51. Based on all of the above, your affiant submits that there is probable cause to believe that YI-LAN CHEN, a/k/a "KEVIN CHEN," has exported and attempted to export U.S. goods to Iran by way of Taiwan and Hong Kong in violation of the IEEPA (Title 50, United States Code, Sections 1701, *et seq.*), the U.S.-Iran Embargo, the ITR, and the EAR.


ALAN BERKOWITZ, SPECIAL AGENT
United States Department of Commerce
Bureau of Industry and Security
Office of Export Enforcement

Sworn to and subscribed before me
On this ~~24~~ day of January 2010


PATRICK A. WHITE
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF FLORIDA