AUSA: Douglas Salzenstein Telephone: (313) 226-9100

AO 91 (Rev. 11/11) Criminal Complaint Special Agent: Richard Foran Telephone: (313) 965-6059

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

14

United States of America
v.
AMIN HASANZADEH

Case:2:19-mj-30572
Judge: Unassigned,
Filed: 10-31-2019 At 01:56 PM
SEALED MATTER (LH)

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(s) of January 2015 through June 2016 in the county of Washtenaw in the Eastern District of Michigan, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 2314, 371	Interstate transportation of stolen property (including conspiracy)
18 U.S.C. § 1546	Fraud and misuse of visas, permits and other documents

This criminal complaint is based on these facts:

See Attached Affidavit.

☑ Continued on the attached sheet.

Complainant's signature

Richard Foran, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/31/19

Judge's signature

City and state: Detroit, Michigan

Mona K. Majzoub, United States Magistrate Judge
Printed name and title

Affidavit in Support of a Criminal Complaint

I, Richard W. Foran, a Special Agent of the Federal Bureau of Investigation (FBI), being duly sworn, depose and state:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since 2015. I am currently assigned to the FBI's Counterintelligence Division, Detroit Field Office, and prior to that, I was assigned to the Violent Crime Task Force in Detroit, giving me both criminal and national security experience. For the last three years, my career has been dedicated to working counterintelligence and counterproliferation investigations involving the illegal transfer of commodities, technologies, information and services from the United States, which are regulated by the U.S. Departments of Commerce, State and the Treasury. I have gained experience in the conduct of such investigations, including, International Emergency Powers Act investigations and International Traffic in Arms Regulations investigations, as well as through formal and informal training, and in consultation with other members of the U.S. federal law enforcement community regarding such matters.

2. My investigative experience as a case agent has aided in the arrest and/or indictment of multiple proliferators and companies for their involvement in the illegal transfer of U.S. origin technologies. Through my training, education, and experience – which has included: debriefing witnesses concerning violations of federal export laws; reviewing financial records that reflect structuring of money orders, deposits and withdrawals; conducting surveillance of individuals engaged in violating federal law; and executing search warrants – I have become familiar with the manner in which commodities are exported from the United States directly or

indirectly to various countries, to avoid both reporting requirements and detection by law enforcement.

3. I make this affidavit in support of an application for a criminal complaint and arrest warrant charging Amin HASANZADEH (hereinafter "HASANZADEH"), an Iranian born citizen who now resides in Michigan and has Lawful Permanent Resident status in the United States, with the following offenses:

a. 18 U.S.C. §§ 2314 and 371 interstate transportation of stolen property (including conspiracy) and;

b. 18 U.S.C. § 1546 fraud and misuse of visas, permits and other documents

4. There is probable cause to conclude that HASANZADEH, between in or about January 2015 and in or about June 2016, within the Eastern District of Michigan and elsewhere, knowingly and willfully stole confidential documents and technical data from his employer, Victim Company A (a company with offices in the Eastern District of Michigan) and thereafter emailed those documents to multiple individuals, including his brother, Sina Hassanzadeh, in Iran, using the Internet (across state or U.S. boundary lines).

5. HASANZADEH has also committed acts in violation 18 U.S.C. 1546, fraud and misuse of visas, permits and other documents, by concealing his military affiliation in Iran from U.S. Citizenship and Immigration Service officials and providing false statements on his I-485 Legal Permanent Resident (LPR) and N-400 Citizenship applications, which HASANZADEH signed and acknowledged under penalty of perjury.

6. The information set forth in this affidavit was obtained during the course of this investigation, including through personal observations, my review of federal agency reports, other documents and other evidence, and from information communicated to me by other law

enforcement officers. Because this affidavit is submitted for the limited purpose of seeking the issuance of a criminal complaint and arrest warrant, it does not include every fact known to me concerning this investigation.

Facts Supporting a Finding of Probable Cause

7. In 1995, the President issued Executive Order (E.O.) 12957, finding that "the actions and policies of the Government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States," and on that date declared a national emergency to deal with that threat.

8. According to immigration and citizenship records, HASANZADEH, who was born in Iran in July 1977, is an Iranian National who currently has LPR status in the U.S (LPR status granted on August 24, 2013). HASANZADEH currently resides in Ypsilanti, Michigan. HASANZADEH has a PhD in Electrical Engineering from Sharif University of Technology (SUT) and a Master's degree in Science in Electrical Engineering from K.N. Toosi University of Technology, Tehran, Iran.

9. As discussed in paragraphs 37 and 41 below, the FBI's investigation also revealed HASANZADEH served in the Iranian military. According to his resumes, prior to arriving in the United States, HASANZADEH also worked at the Iranian company, Basamad Azma. The website www.IranWatch.org contained a 2005 report that indicated that Basamad Azma is affiliated with the Iranian government's Cruise Division of Air & Space Organization.

10. From approximately 2011-2013, HASANZADEH worked as a research faculty member at Florida State University's Center for Advanced Power Systems— a Cleared Defense Contractor—where he specialized in developing power electronics computer designs, modeling

and simulation, analog/digital electronics and control systems designation. During 2013-2014, HASANZADEH conducted similar research at the University of Maryland's Power Electronics, Energy Harvesting and Renewable Energies Laboratory (PEHREL), within the Department of Electrical and Computer Engineering.

11. HASANZADEH married "Person A" in October 2014. Person A is an Iranian national admitted to the U.S. on an F-1 student visa in or about August 2013. Person A was accepted into the doctoral program in the Electrical Engineering Department at the University of Michigan and was awarded a PhD in or about late 2018.

12. Prior to her U.S. entry, Person A received a Bachelor of Science degree from Shahid Behesti University and a Master's of Science in Electronics from the SUT, Tehran, Iran, with an emphasis in micro-electronics and circuit design.

13. HASANZADEH has a brother by the name of Sina Hassanzadeh (hereinafter "Sina"). Sina is an Iranian citizen living in Iran with an identified date of birth of XXXXXX XX, 1986. According to his resume, Sina was also educated at SUT and obtained a Masters of Science degree in Electrical Engineering.

14. Sina's resumes highlight his expertise in hardware engineering and experience programming code with the Iranian company, Kavosh Samaneh Ayria, based in Tehran, Iran. Sina's resume also shows his employment with several Iranian companies that are of proliferation concern. For example, Sina worked for Basamad Azma Company from 2009-2010, an entity affiliated with Iran's cruise missile research. Sina was also employed with the Iranian companies Moj Pardaz and Bashir, between 2013 and 2018. Indeed, Sina's job responsibilities are indicative of military programs. The Bashir Industrial Complex is an entity that contributes to

Iran's proliferation-sensitive nuclear activities and/or its development of nuclear weapons or their delivery systems. Bashir is co-owned by Iran Electronics Industries (IEI) and Iran Aircraft Manufacturing Company (HESA), under the Ministry of Defense and Armed Forces Logistics.

HASANZADEH's employment with Victim Company A

15. On or about January 12, 2015, HASANZADEH began employment with Victim Company A as a senior hardware engineer (here in the Eastern District of Michigan). Victim Company A has domestic and international clients in the automotive and aerospace industries.

16. As a senior hardware engineer, HASANZADEH was given access to Victim Company A's highly sensitive confidential and proprietary information in the form of schematics, layouts, designs, projects, diagrams, performance reports and other documents and data. HAZANZADEH'S responsibilities, in fact, included work on two projects of significant value to Victim Company A, including one of the company's most sensitive projects (described as a real-time supercomputer with applications that would include aerospace applications). This project involved documents that were not disseminated to the public and had research and development involving millions of dollars.

17. Accordingly, many of the documents that HASANZADEH had access to as part of his employment were marked as being confidential and not to be distributed or duplicated without permission.

18. Indeed, according to a senior hardware engineer employed by Victim Company A, senior hardware engineers like HASANZADEH were not permitted to take work home and were not allowed to use personal email accounts to transfer data. According to this same

individual, hardware engineers were aware, moreover, that they should not transfer work to a personal computer without prior approval by Victim Company A.

19. Victim Company A protected its confidential and proprietary documents and information by entering into Non-Disclosure Agreements (NDAs) with its customers and collaborative partners.

20. Victim Company A further protected its confidential and proprietary documents and data by entering into employee agreements with engineers like HASANZADEH when they began working for Victim Company A. For example, Paragraph 3.0 of HASANZADEH'S signed Employee Agreement informed HASANZADEH that, both during and after his employment, he could not use or disclose, directly or indirectly, for his own benefit or for the benefit of another, any trade secret (as defined), except to the extent authorized by Victim Company A.

21. HASANZADEH also agreed, as part of his Employee Agreement, that upon termination of his employment, he was to deliver to Victim Company A all of its property in his possession (including but not limited to, all records, documents, hardware, software and all copies).

22. Paragraph 4.0 of the Employee Agreement also informed HASANZADEH that he was also prohibited from disclosing any information which was confidential to any of Victim Company A's customers, partners or joint venture partners, except as required in connection with his duties on behalf of Victim Company A. Paragraph 4.0 was critical because, as part of its business, Victim Company A received confidential, proprietary and trade secret documents from others, including its customers and collaborative partners. A senior company official advised that

any unauthorized disclosure or theft of partner company documents and information protected under an NDA could be "catastrophic."

HASANZADEH illegally and covertly transfers proprietary, trade secret and/or confidential documents belonging to Victim Company A and its customers/partners to Sina in Iran

23. Investigation has revealed that, even before his employment with Victim Company A, Hasanzadeh begin communicating with Sina about Hasanzadeh's potential employment with Victim Company A. For example, on or about November 15, 2014, HASANZADEH sent an email communication to Sina with the subject line: "Fwd: [Victim Company A] Hardware Engineer." This email contained notification of a job description for Victim Company A's Hardware Engineering Team, which included technical position requirements and preferred experience, along with Victim Company A's website. On or about December 18, 2014, HASANZADEH emailed Sina a suggested reading list that he received for his prospective employment with Victim Company A, which included technology architecture, specifications and platforms associated with Victim Company A. Two days later, on December 20, 2014, HASANZADEH forwarded Victim Company A's project data to Sina with the subject line: "We need to talk." I believe, based on my training and experience, that HASANZADEH was sending these emails (prior to employment) to identify that if he was hired as a hardware engineer, he would have access to technologies and projects of interest to Sina and/or Sina's Iranian employers.

24. After obtaining employment with Victim Company A, HASANZADEH was assigned to projects that suited his unique hardware engineering skill set. These projects contained Victim Company A's highly sensitive confidential and proprietary documents in the form of schematics, layouts, designs, projects, diagrams, performance reports and other

documents, and were subject to company NDAs. As discussed above, HASANZADEH had access to hardware engineering project documents that, according to interviews with Victim Company A officials, were highly sensitive projects, that were not available to the public, were marked as confidential and were not to be distributed or duplicated without company permission.

25. Investigation has revealed, however, that only six days after he began employment with Victim Company A, HASANZADEH began covertly transferring Victim Company A's project documents and data as well as confidential documents that Victim Company A had received from its partners/customers, to Sina's email account in Iran. HASANZADEH concealed these communications from Victim Company A by almost exclusively using a personal email account to transfer documents to Sina. These unauthorized transfers occurred on a regular basis and continued until approximately June 11, 2016. These transfers included hundreds of Victim Company A layouts, projects, schematics, notes, zip files and other documents and data, emailed by HASANZADEH to Sina without Victim Company A's knowledge or consent.

26. For example, on or about January 18, 2015, HASANZADEH sent an email to and from one of his personal email accounts with the subject line: "Data Sheet." The email contained four document attachments. On the same date, HASANZADEH forwarded these four documents, along with an additional document, to Sina (again using his personal email account). In the body of the email, HASANZADEH identified specific pages of interest.

27. Victim Company A officials reviewed and confirmed that these documents contained product performance specifications, confidential information belonging to other partner engineering companies, and/or proprietary information belonging to them, which were

not available to the general public. Specifically, one attachment was marked "Confidential" information belonging to an identified U.S. partner company and the another attachment was marked "NDA Confidential" property belonging to Victim Company A, meaning it involved a NDA with a partner company.

28. Similarly, on or about May 8, 2015, HASANZADEH used a personal email account to send an email to Sina with the subject: "Sch" that contained two "zip" file attachments. These "zip" files contained numerous folders with sensitive proprietary technical documents and data belonging to Victim Company A. On or about May 17, 2015, HASANZADEH transferred other technical drawings.

29. According to company officials, the technical drawings and schematics transferred by HASANZADEH using his personal email account were critical to the development and use of one of Victim Company A's most important projects. Both drawings were clearly marked as confidential.

30. A senior company official stated the documents related to projects developed by Victim Company A and were considered trade secret. These projects underwent "months" of engineering development and testing before they were introduced to the market and were extremely valuable to the company. The company official stated these projects were subject to NDAs and the transfer of these drawings/schematics to Sina would have enabled Sina to replicate the designs.

31. Likewise, on or about May 20, 2015, HASANZADEH sent Sina an email that contained a 1.3MB attachment (again using a personal email account). The attached document was specifically authored by HASANZADEH and marked by HASANZADEH as being

"[Victim Company A] Confidential Document, Not To Be Distributed or Duplicated Without Permission." According to company officials, HASANZADEH, being the author of the document, would have had to personally label the technical report as confidential. Company officials described the document as a highly detailed, functional specification report and a trade secret.

32. Investigation revealed that HASANZADEH continued to illegally transfer sensitive project documents and data belonging to Victim Company A and/or its partners/customers via personal email to Sina through 2016.

33. Email subscriber information showed that the email account to which HASANZADEH transferred documents to Sina was created by Sina on November 18, 2008 in Iran. A review of Sina's email account activity between 2008 and 2018 confirms logins and updates were made from Iranian Internet Protocol (IP) addresses. In addition to the Iran-based log-in activity, Sina stated, on multiple resumes, that he maintained a physical address in Tehran, Iran on Ashrafi Esfahani Avenue and had an Iranian telephone number. According to these resumes, Sina was also employed in Iran by multiple Iranian companies, identified as Moj Pardaz, Bashir, and Rayan Nik, between 2013 and 2018.

34. On or about April 11, 2016, HAZANZADEH also used his personal email account to transfer a Victim Company A trade secret to Person A, specifically a 13-page technological performance evaluation report related to the development of a prototype electronic component for a high-speed digital board for one of Victim A's important products. The first page of the document was marked "[Victim Company A] Confidential Document, Not To Be

Distributed or Duplicated Without Permission." Company officials advised that HASANZADEH was not authorized to transfer or share this document with Person A.

35. Investigation revealed that HASANZADEH transferred this same document to Sina on April 10, 2016, at 1:10 PM.

36. Investigation has also revealed that at the time of HASANZADEH's illegal transfers of stolen documents, Person A was enrolled as a doctoral student at the University of Michigan. Person A was issued a university email account which provided her cloud storage capability. Investigation revealed the existence of thousands of Victim Company A documents in Person A's cloud storage that is associated with her University of Michigan email account. These files were identified as, but not limited to, internal company component lists, schematics, diagrams, and other project reports marked as confidential. These documents were not generally known to the public and were not ascertainable by Person A through proper means.

18 U.S.C. § 1546 fraud and misuse of visas, permits and other documents

37. In or about October 2010, HASANZADEH completed a U.S. State Department visa application to legally enter the U.S. and attend Florida State University as an engineering student. The application asked "Have you ever served in the military?" HASANZADEH responded "Yes" and listed the branch of service as "Army", the Rank/Position as "Lieutenant", the Military Specialty as "Air Force" and dates of service from February 20, 2002, to December 20, 2003. The application was adjudicated by the U.S. Department of State on or about December 28, 2010, the visa was issued and HASANZADEH was admitted entry to the U.S.

38. However, in or about February 24, 2013, HASANZADEH completed and signed Immigration Form I485, which is an application to register for LPR status in the U.S. In the

application, Part 3, Question 15, HASANZADEH answered "No" to the following question: "Have you ever served in, been a member of, assisted in, or participated in any military unit, paramilitary unit, police unit, self defense unit, vigilante unit, rebel group, guerilla group, militia or insurgent organization?." Under the "Applicant's Statement", Part 5 of the form, HASANZADEH signed and certified under penalty of perjury that the information he provided in the application was all true and correct.

39. On March 7, 2018, HASANZADEH was interviewed at his residence by an official from U.S. Citizenship and Immigration Services in conjunction with Person A's application for LPR status. In that interview, HASANZADEH made oral and written statements about his background, to include military service. In a signed, written statement, HASANZADEH denied having military service in Iran. HASANZADEH crossed out all questions related to military service in this record of sworn statement and wrote "N/A", meaning not applicable.

40. On or about May 29, 2018, HASANZADEH completed Immigration Form N400, Application for Naturalization. Part 12, Question 15 asked if the applicant (HASANZADEH) was "ever a member of or ever served in, help or otherwise participate in any of the following groups: military unit, paramilitary unit, police unit, self defense unit, vigilante unit, rebel group, guerilla group, militia or insurgent organization. HASANZADEH answered "No" to all of the above groups. Part 12, Question 19 asked if HASANZADEH did ever "receive any type of military, paramilitary or weapons training?." HASANZADEH answered "No." HASANZADEH signed the N400 application, under penalty of perjury, on May 29, 2018.

41. In addition to his 2010 admissions, investigation revealed that on or about December 25, 2014, HASANZADEH, using a personal email account, emailed himself seven attachments containing a copy of HASANZADEH's Iranian passport, his Iranian military identification card, a photograph of HASANZADEH in military uniform and other documents.

42. Therefore, HASANZADEH's denial of military service on multiple U.S. immigration applications represents fraud and the intentional provision of false and/or misleading information for him to obtain LPR and naturalization status.

Request for a Criminal Complaint and Arrest Warrant

43. Based upon my experience, training, and the totality of circumstances in the above information, there is probable cause believe that between at least January 2015 and June 2016, HASANZADEH violated 18 U.S.C. §§ 2314, 371 and 1546.

WHEREFORE, I respectfully request that the Court issue a criminal complaint and corresponding arrest warrant charging Amin HASANZADEH for violations of 18 U.S.C. §§ 2314 and 371 Interstate Transportation of Stolen Property (including conspiracy) and 18 U.S.C. § 1546 fraud and misuse of visas, permits and other documents.

Richard W. Foran
Special Agent
Federal Bureau of Investigation

Sworn to before me this
31st day of October 2019

Mona K. Majzoub
United States Magistrate Judge
Eastern District of Michigan