

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA)	
)	
v.)	CRIMINAL NO. 1:15CR124
)	
SOHAIB AKHTER,)	Honorable T.S. Ellis, III
)	
Defendant.)	
)	

STATEMENT OF FACTS

The parties stipulate and agree that the allegations in Counts One, Two, and Eight of the Indictment and the following facts are true and correct, and that had the matter gone to trial the United States would have proven them beyond a reasonable doubt.

1. Between in or about March 2014, and continuing thereafter until in or about April 2015, in the Eastern District of Virginia and elsewhere, the defendant, SOHAIB AKHTER, knowingly and willfully conspired with persons known and unknown, including Muneeb Akhter and Musaddiq Ishaq, to devise, execute, and attempt to execute a scheme and artifice to defraud Expedia, Inc., U.S. Airways, Beezid Inc., OvernightPrints.com, TechConnect, and others (hereinafter "Vendors"), to obtain money and property by means of false and fraudulent pretenses, representations, and promises, and caused the transmission of certain writings and signals in interstate commerce for the purpose of executing such scheme or artifice to defraud, in violation of Title 18, United States Code, Sections 1343 and 1349.

2. It was a part of the conspiracy and scheme to defraud that SOHAIB AKHTER and coconspirators would steal from Victim Company 1, an Internet-based cosmetics company,

credit card account information belonging to Victim Company 1's customers, who were individuals located throughout the United States and abroad (collectively "the identity theft victims").

3. SOHAIB AKHTER and coconspirators would use the stolen information, which included compromised credit card numbers, along with the names, addresses, phone numbers, and email addresses of the identity theft victims (hereinafter "means of identification"), to make purchases from the Vendors, which were located throughout the United States and abroad.

4. In or about April 2014, in Sterling, Virginia, in the Eastern District of Virginia, Muneeb Akhter secretly installed a computer code onto the computer system of Victim Company 1. The code automatically emailed the credit card numbers and means of identification of the identity theft victims to email accounts controlled by Muneeb Akhter, who provided SOHAIB AKHTER and coconspirators with the information upon request.

5. SOHAIB AKHTER and coconspirators were familiar with Victim Company 1 because Ishaq's mother, T.U., was the owner of the Company.

6. SOHAIB AKHTER and coconspirators made purchases via the Internet on the Vendors' websites.

7. SOHAIB AKHTER and coconspirators caused many of the goods that they purchased from the Vendors using the identity theft victims' stolen credit card numbers and means of identification to be delivered to the AKHTER residence.

8. SOHAIB AKHTER and coconspirators resold and attempted to resell goods and services that they purchased with the identity theft victims' information on websites including, but not limited to, Craigslist.com.

9. SOHAIB AKHTER and coconspirators used stolen credit card numbers and means of identification to purchase goods and services both before and after law enforcement agents contacted Muneeb Akhter and SOHAIB AKHTER and executed a federal search warrant at their home on or about July 24, 2014.

10. SOHAIB AKHTER and coconspirators used or attempted to use stolen credit card numbers and means of identification belonging to more than 40 individuals to purchase goods and services.

11. Fraudulent purchases attributed to SOHAIB AKHTER and coconspirators affected more than 20 businesses.

12. The total loss amount associated with the conspirators' credit card scheme exceeded \$30,000.

13. In addition, SOHAIB AKHTER and coconspirators attempted numerous fraudulent transactions that were halted by fraud protection methods.

14. On or about each of the dates set forth below, in the Eastern District of Virginia and elsewhere, SOHAIB AKHTER and coconspirators, for the purpose of executing the scheme described above, and attempting to do so, caused to be transmitted by means of wire communication in interstate commerce the signals and sounds described below.

Date	Description	Cardholder/Credit Card No.	Loss Amount
5/9/2014	Electronic purchase of Beedzid Bid Pack on website Beezid.com	L.L./-7882	\$550.00
5/16/2014	Electronic purchase of marketing materials on website OvernightPrints.com	L.L./-7882	470.17

5/19/2014	Electronic purchase of marketing materials on website OvernightPrints.com	A.H./-0110	\$697.03
5/26/2014	Electronic purchase of hotel room and rental car on website Expedia.com	D.F./-1681	\$641.41
5/26/2014	Electronic purchase of flight, hotel room, and rental car on website Expedia.com	J.R./-6665	\$641.41
5/28/2014	Electronic purchase of flight on website of U.S. Airways	D.G./-5096	\$816.00
6/16/2014	Electronic purchase of conference attendance on website of TechConnect	F.K./-9916	\$795.00
6/16/2014	Electronic purchase of conference attendance on website of TechConnect	J.H./-4748	\$795.00

15. Furthermore, between in or about March 2014, and continuing thereafter until in or about March 2015, in the Eastern District of Virginia and elsewhere, the defendant, SOHAIB AKHTER, knowingly and intentionally conspired and agreed with others known and unknown, including Muneeb Akhter and Ishaq, to commit an offense against the United States, that is, to knowingly and intentionally access a computer without authorization and exceed authorized access to a computer, and thereby obtain information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain, and the offense was committed in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, wire fraud, in violation of Title 18, United States Code, Section 1343, as charged in Count One of the Indictment, and the value of the information obtained exceeded \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and (c)(2)(B)(i)-(iii) and 371.

16. In or about March 2014, in Sterling, Virginia, in the Eastern District of Virginia, SOHAIB AKHTER, Muneeb Akhter, Ishaq, and others met in the warehouse of Victim Company 1. During the meeting, SOHAIB AKHTER and Muneeb Akhter stated a desire to hack websites in order to steal credit card information.

17. Muneeb Akhter would and did surreptitiously install at least one keystroke logger on a computer used by employees of Victim Company 1 with the purpose of accessing and altering the system of computers belonging to Victim Company 1.

18. Through the use of at least one keystroke logger, Muneeb Akhter would and did obtain the user name and password belonging to at least one employee of Victim Company 1.

19. In or about April 2014, Muneeb Akhter created the email account credproc@hotmail.com. In or about June 2014, Muneeb Akhter created the email account nsallookup@hotmail.com. SOHAIB AKHTER was familiar with these accounts and understood that they were created in furtherance of the conspiracy to use stolen credit card numbers and means of identification to purchase goods and services.

20. In or about April 2014, in Sterling, Virginia, in the Eastern District of Virginia, Muneeb Akhter used an employee's username and password, which he had stolen with the use of keystroke logger software, to gain access to Victim Company 1's computer system. Muneeb Akhter then surreptitiously installed a computer code on Victim Company 1's website that caused the identity theft victims' information to be sent in emails to credproc@hotmail.com.

21. The code caused the website to collect information from the online checkout page of Victim Company 1's website. The collected information included credit card numbers and means of identification belonging to the identity theft victims, who had purchased items on Victim Company 1's website.

22. The code sending information to credproc@hotmail.com caused technical problems on Victim Company 1's website. T.U. hired a specialist to investigate and the specialist removed the malicious code.

23. In or about June 2014, in Sterling, Virginia, in the Eastern District of Virginia, Muneeb Akhter installed a second computer code on Victim Company 1's website. The second code was more difficult to detect than the first code and did not cause obvious technical problems. The new code caused Victim Company 1's website to email the identity theft victims' information to nsalookup@hotmail.com.

24. From on or about June 3, 2014 through on or about July 24, 2014, SOHAIB AKHTER, Muneeb Akhter, Ishaq, and coconspirators collected credit card numbers and means of identification derived from approximately 3,000 transactions on Victim Company 1's website in the nsalookup@hotmail.com account.

25. In or about mid-July 2014, a reporter informed SOHAIB AKHTER and Muneeb Akhter about the existence of an unexecuted state search warrant for their residence. SOHAIB AKHTER and Muneeb Akhter erased the contents of their computers and the nsalookup@hotmail.com and credproc@hotmail.com accounts with the purpose of preventing law enforcement from examining them.

26. Although SOHAIB AKHTER and Muneeb Akhter erased the contents of nsalookup@hotmail.com in or about mid-July 2014, the account continued to collect new credit card numbers and means of identification from the Victim Company 1 website until Victim Company 1 removed the code in or about May 2015.

27. Furthermore, between in or about June 2014, and continuing thereafter until in or about March 2015, in the Eastern District of Virginia and elsewhere, the defendant, SOHAIB

AKHTER, knowingly and intentionally conspired and agreed with others known and unknown, including Muneeb Akhter and Ishaq, to commit an offense against the United States, that is, to knowingly and intentionally access a computer without authorization and exceed authorized access to a computer, and thereby obtain information from a department and agency of the United States, and the offense was committed for purposes of commercial advantage and private financial gain, and the offense was committed in furtherance of a criminal and tortious act in violation of the laws of the Commonwealth of Virginia, specifically, Computer Invasion of Privacy, in violation of Va. Code Ann. § 18.2-152.5, and the value of the information obtained exceeded \$5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(B) and (c)(2)(B)(i)-(iii) and 371.

28. It was part of the conspiracy that SOHAIB AKHTER, Muneeb Akhter, Ishaq, and other coconspirators known and unknown, engaged in a series of computer intrusions and attempted computer intrusions against the State Department to obtain sensitive passport and visa information and other related and valuable information about State Department computer systems.

29. On or about June 24, 2014, Muneeb Akhter and SOHAIB AKHTER had the following conversation soon after Muneeb Akhter was hired to work as an Information Technology Security Specialist at the Department of Homeland Security:

SOHAIB AKHTER: You gotta case the joint. You gotta figure out exactly what's happening here and there and have an elaborate scheme built out that you'll never leave a trace.

Muneeb Akhter: Yeah, you first climb the ladder before you Know your shit. Need to know who's watching, what they're watching, and luckily I'm one of the people that are watching, so I know what kind of evades.

SOHAIB AKHTER: Yeah, but I'm pretty sure they have insider protection methods and you gotta figure that shit out.

Muneeb Akhter: Yeah.

SOHAIB AKHTER: Best not to be the first person to do shit. See around, do it for probably a year or so, make sure that other people

Muneeb Akhter: We get access to a lot of different viruses, malware strains, just because you're watching the packets and you see that this thing is malicious and you can download their binaries, their weird malware. Wonder if you could really retool it such that it becomes a weapon on your part.

30. In or about October 2014, SOHAIB AKHTER was hired by ActioNet, Inc. (hereinafter "ActioNet") to perform information technology support for the State Department.

31. From in or about October 2014 to in or about February 2015, SOHAIB AKHTER was assigned to a contract position within the Bureau of Consular Affairs (hereinafter "Bureau"), a division of the State Department, which administers laws, formulates regulations, and implements policies relating to consular services and immigration. SOHAIB AKHTER performed his duties at both ActioNet offices in Falls Church, Virginia, in the Eastern District of Virginia, and Bureau offices in Washington, DC, which were located in a building called SA-17.

32. SOHAIB AKHTER used his contract position at the State Department to search for and access sensitive passport information belonging to coworkers, acquaintances, a former employer, and federal agents investigating him for crimes alleged in the Indictment.

33. After accessing sensitive passport information from State Department computers, SOHAIB AKHTER copied, saved, and shared this information with coconspirators.

34. Beginning on or about February 12, 2015, and continuing thereafter until on or about February 19, 2015, in Falls Church, Virginia, in the Eastern District of Virginia, and

elsewhere, SOHAIB AKHTER, accessed a Bureau database called Passport Lockbox (hereinafter "Lockbox") without authorization.

35. Lockbox was a Bureau program that performs payment processing, scanning of applications, and initial data entry for U.S. passport applications. Lockbox has a computer database containing imaged passport applications associated with real individuals. The imaged passport applications in Lockbox's database contain, among other things, a photograph of the passport applicant, as well as certain personal information including the applicant's full name, date and place of birth, current address, telephone numbers, and parent information.

36. Prior to accessing the Lockbox database, and throughout his tenure as a contractor with the State Department, SOHAIB AKHTER was made aware of and indicated he understood: (a) the confidential nature of the Lockbox database and the confidential personal data contained therein; (b) the information contained in the passport records maintained by the State Department pursuant to Lockbox is protected from unauthorized disclosure by the Privacy Act of 1974, 5 U.S.C. § 552a; and (c) passport applications maintained by the State Department in the Lockbox database should be accessed only in connection with an employee's official government duties and not the employee's interest or curiosity.

37. At all times relevant hereto, upon logging onto a State Department computer, the following warning banner was displayed to the user:

You are accessing a U.S. Government information system, which includes (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

38. The banner also provided the user with a warning that he/she had “no reasonable expectation of privacy regarding any use” of the system and that all computer activity was subject to monitoring and retrieval by State Department and law enforcement officials. To gain access to a State Department computer, SOHAIB AKHTER was required to click the icon marked “OK.”

39. Furthermore, the Lockbox Report Parameter Form, which SOHAIB AKHTER used to search for and access passport information, warned the user that the database contained “Sensitive But Unclassified” material. A banner further stated:

This information *shall be considered confidential* Access to and use of such information must be solely for the formulation, amendment, administration, or enforcement of the immigration, nationality, and other laws of the United States Do not access this information in anything other than an official capacity, and do not share it without the permission of the Department of State.

40. Between on or about February 12, 2015, and on or about February 19, 2015, SOHAIB AKHTER conducted approximately 119 unauthorized searches for U.S. passport records using the Passport Lockbox Lookup report. He accessed personal passport information for approximately 62 different individuals without authorization. Those individuals included: G.R., a DHS special agent investigating the crimes alleged in the Indictment; A.M., the CEO of Victim Company 2; Muneeb Akhter; Ishaq; and himself. In addition, SOHAIB AKHTER attempted to access passport information for S.T., a DHS special agent investigating the crimes alleged in the Indictment.

41. In or about February 2015, SOHAIB AKHTER copied and removed the personal passport information associated with several of these individuals, including DHS Special Agent G.R., without authorization.

42. On or about February 20, 2015, SOHAIB AKHTER had the following conversation with special agents of the State Department about accessing individuals' personal passport information:

Special Agent R.M.: Was this part of your normal duties, or was this going above and beyond to figure out processes?

SOHAIB AKHTER: I was trying to figure out how the system works, yes. It was slightly above going above and beyond, but that's kind of my nature, trying to trouble shoot an issue to its fullest extent and show how things work . . . and understand the database so at some time provide the services with or without ActioNet's support to the [State Department], whoever I may be working for so I could understand the system, properly construct a proposal and submit that for consideration for a contract.

Special Agent R.M.: So I understand this correctly, this is not part of your job. You were trying to understand the system, and doing your own research on how the system works?

SOHAIB AKHTER: Yes.

[. . .]

Special Agent R.M.: Do you have any intention while working at State Department to take any known PII [personal identifying] information or introduce anything into our system?

SOHAIB AKHTER: I have no ill intentions of using anyone's personal information within the system, certainly not.

43. In or about February 2015, SOHAIB AKHTER downloaded several programs to a State Department computer without authorization. These programs included malicious software, or malware.

44. In or about February 2015, SOHAIB AKHTER told Ishaq that if he was able to gain remote access to State Department computer systems, he could: access information on individuals' passport applications; access and unilaterally approve visa applications without State Department authorization in exchange for payment; and create passports and visas and sell them.

45. In or about February 2015, SOHAIB AKHTER learned that he was being transferred to a new position by ActioNet and would no longer have access to SA-17. SOHAIB AKHTER knew that he would lose the ability to access certain Bureau computer servers once he was transferred. As a result, SOHAIB AKHTER put into motion a plan to ensure that he could maintain access to desired Bureau servers even after he was transferred out of SA-17 and even if he no longer worked at the State Department.

46. SOHAIB AKHTER orchestrated a scheme to secretly install a physical device at SA-17. Once installed, the device would enable SOHAIB AKHTER and coconspirators to collect data from and remotely access State Department computer systems.

47. SOHAIB AKHTER led the conspiracy, organized the intrusion to install the physical device, recruited coconspirators to assist in execution of the intrusion, and managed the execution of the intrusion.

48. Muneeb Akhter provided technical assistance to SOHAIB AKHTER for the unauthorized access. Muneeb Akhter programmed the physical device, known as a "gumstix," so that it would collect data from State Department computers and be utilized to transmit it to computers controlled by Muneeb Akhter and SOHAIB AKHTER and coconspirators.

49. On the day the scheme was executed, Ishaq transported materials, including the gumstix, from Muneeb Akhter, located at the AKHTER residence, to SOHAIB AKHTER, located at SA-17.

50. On or about February 15, 2015, SOHAIB AKHTER called Ishaq and asked him to buy a drill. Ishaq purchased the drill and then, pursuant to SOHAIB AKHTER's request, drove to the AKHTER residence to pick up additional items from Muneeb Akhter. At the AKHTER residence, in Springfield, Virginia, in the Eastern District of Virginia, Muneeb Akhter

was in the process of programming a SD card, which was later to be inserted into the gumstix. Muneeb Akhter gave Ishaq a bag containing a screwdriver, tape, glue, and the gumstix. Pursuant to SOHAIB AKHTER's request, Ishaq drove to SA-17, in Washington, DC, and delivered the bag and items to SOHAIB AKHTER outside SA-17. Later that day, Muneeb Akhter drove separately to Washington, DC, and delivered the programmed SD card to SOHAIB AKHTER.

51. SOHAIB AKHTER took all of the materials provided by Ishaq and Muneeb Akhter into a room inside SA-17. SOHAIB AKHTER removed a panel on a wall and attempted to drill a hole in the metal siding. SOHAIB AKHTER planned to run wires through the hole in order to connect the gumstix to Bureau servers and the building's power supply. SOHAIB AKHTER planned to install the gumstix and the attached cables behind the wall in such a way that the device would be undetectable.

52. SOHAIB AKHTER lacked the proper tools to drill through the metal siding. In addition, SOHAIB AKHTER broke the power regulator for the device while attempting to install it within the wall. For these reasons, SOHAIB AKHTER was forced to abandon the conspirators' plan to install the device.


53. On or about the evening of February 15, 2015, SOHAIB AKHTER called Muneeb Akhter and told him that he attempted to install the gumstix behind a wall inside SA-17 but was ultimately unsuccessful.

54. The acts taken by the defendant, SOHAIB AKHTER, in furtherance of the offenses charged in this case, including the acts described above, were done willfully and knowingly with the specific intent to violate the law. The defendant acknowledges that the foregoing Statement of Facts does not describe all of the defendant's conduct relating to the offenses charged in this case nor does it identify all of the persons with whom the defendant may


have engaged in illegal activities. The defendant further acknowledges that he is obligated under his plea agreement to provide additional information about this case beyond that which is described in this Statement of Facts.

55. The Statement of Facts shall be admissible as a knowing and voluntary confession in any proceeding against the defendant regardless of whether the plea agreement is presented to or accepted by a court. Moreover, the defendant waives any rights that the defendant may have under Fed. R. Crim. P. 11(f), Fed. R. Evid. 410, the United States Constitution, and any federal statute or rule in objecting to the admissibility of the Statement of Facts in any such proceeding.

Dana J. Boente
United States Attorney

By: 

John P. Taddei
Special Assistant United States Attorney (LT)

By: 

Jennifer A. Clarke
Special Assistant United States Attorney (LT)

Defendant's Stipulation and Signature


After consulting with my attorney and pursuant to the plea agreement entered into this day between the defendant, SOHAIB AKHTER, and the United States, I hereby stipulate that the above Statement of Facts is true and accurate, and that had the matter proceeded to trial, the United States would have proved the same beyond a reasonable doubt.



SOHAIB AKHTER
Defendant

Defense Counsel's Signature

I am Gadeir Abbas, the attorney for SOHAIB AKHTER. I have carefully reviewed the above Statement of Facts with him. To my knowledge, his decision to stipulate to these facts is informed and voluntary.



Gadeir Abbas, Esq.
Attorney for SOHAIB AKHTER