IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	)	CRIMINAL NO. 1:15CR124
	)	
v.	)	Count 1: Conspiracy to Commit Wire Fraud
	)	(18 U.S.C. § 1349)
MUNEEB AKHTER	)	
SOHAIB AKHTER,	)	Count 2: Conspiracy to Access a Protected
	)	Computer without Authorization
Defendants.	)	(18 U.S.C. § 371)
	)	
	)	Counts 3-6: Aggravated Identity Theft
	)	(18 U.S.C. § 1028A)
	)	
	)	Count 7: Access of a Protected Computer
	)	without Authorization
	)	(18 U.S.C. § 1030(a)(2))
	)	
	)	Count 8: Conspiracy to Access a
	)	Government Computer without
	)	Authorization
	)	(18 U.S.C. § 371)
	)	
	)	Counts 9-11: False Statements
	)	(18 U.S.C. § 1001)
	)	
	)	Count 12: Obstruction of Due
	)	Administration of Justice
	)	(18 U.S.C. § 3147)
	)	
	)	Forfeiture Notice

INDICTMENT

April 2015 Term – at Alexandria, Virginia

THE GRAND JURY CHARGES THAT

COUNT ONE

(Conspiracy to Commit Wire Fraud)

Introductory Allegations

At all times relevant to this Indictment:

1. Victim Company 1, known to the Grand Jury, is an Internet-based cosmetics company. Its offices and computer systems are located in Sterling, Virginia, in the Eastern District of Virginia.

2. Defendants MUNEEB AKHTER and SOHAIB AKHTER maintained a residence located in Springfield, Virginia, in the Eastern District of Virginia (hereinafter "AKHTER residence").

3. Expedia, Inc. maintains several global online travel brands, including Expedia.com. Its headquarters are located in Bellevue, Washington.

4. U.S. Airways is an American airline. Its headquarters are located in Tempe, Arizona.

5. Beezid Inc. maintains Beezid.com, an online auction website. Its headquarters are located in Montreal, Quebec, Canada.

6. OvernightPrints.com produces printed materials, including business cards and brochures. Its headquarters are located in Las Vegas, Nevada.

7. TechConnect is a global technology outreach and development organization that hosts conferences worldwide. Its headquarters are located in Austin, Texas.

The Conspiracy

8. Between in or about March 2014, and continuing thereafter until in or about April 2015, in the Eastern District of Virginia and elsewhere, the defendants, MUNEEB AKHTER and

SOHAIB AKHTER, knowingly and willfully conspired together, and with persons known and unknown to the Grand Jury, including unindicted coconspirator 1 (hereinafter UCC-1), 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, Section 1343.

MANNER AND MEANS OF THE CONSPIRACY

It was a part of the conspiracy and scheme to defraud that:

9. MUNEEB AKHTER and SOHAIB AKHTER and coconspirators would steal from Victim Company 1 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").

10. MUNEEB AKHTER and SOHAIB AKHTER and coconspirators were familiar with Victim Company 1 because UCC-1's mother, T.U., was the owner of the Company.

11. MUNEEB AKHTER and 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.

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

13. MUNEEB AKHTER and 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.

14. MUNEEB AKHTER and 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.

15. MUNEEB AKHTER and SOHAIB AKHTER and coconspirators attempted numerous fraudulent transactions that were halted by fraud protection methods.

OVERT ACTS

In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere:

16. On or about June 26, 2014, in Washington, DC, in a sworn written statement, MUNEEB AKHTER told a Department of Homeland Security (hereinafter "DHS") special agent that he had created a computer code to gain unauthorized access to several websites including K-Mart, Shell Gasoline, Whole Foods, Starbucks, and Dunkin' Donuts. MUNEEB AKHTER swore that he "successfully used [his] script to conduct DNS spoofing attacks," a type of computer hack, which allowed him to "trick the [companies' computer] system[s] into thinking [he was] reloading gift cards with actual money," even though he was not expending any money to load the cards. He admitted to using the gift cards for personal use, as well as fraudulently placing value on gift cards for others, also without expending money.

17. On or about July 15, 2014, SOHAIB AKHTER told UCC-1 that the code MUNEEB AKHTER described to the DHS agent did not exist.

18. 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 and SOHAIB AKHTER.

19. On or about May 27, 2014, SOHAIB AKHTER and UCC-1 had the following conversation:

UCC-1: Did it work man?

SOHAIB AKHTER: What? Yeah, he's on the plane man.

UCC-1: Damn! Yo, that is insane! So, he printed it out, everything worked?

SOHAIB AKHTER: Yep.

UCC-1: Damn boy, that's legit! We could fly in England man.

SOHAIB AKHTER: Dude, don't do international, just stay here. You go international, you got to provide a passport and shit, and if something don't turn out right, you know, it's horrible to stay in another country.

[. . .]

SOHAIB AKHTER: I mean, let's see if it works, 'cause other places won't even know, you know, what to do with fraud. America is more hardened to, you know, what will happen if somebody steals someone else's credit card. But in other countries, I don't know if they know.

UCC-1: Yeah. I don't know if they know anything dude. That's legit though man.

SOHAIB AKHTER: But, Inshallah, he gets his hotel and car too.

20. On or about May 28, 2014, SOHAIB AKHTER and UCC-1 had the following conversation:

SOHAIB AKHTER: They're trying to crack down on card fraud. It's like, you know, it shouldn't be happening. It's only dumb people that are duped. People who haven't created their systems right.

UCC-1: Yeah.

SOHAIB AKHTER: [. . .] I can't believe Expedia, like I thought Expedia was one of the big companies, they would definitely know cc fraud if they saw it, you know. But they were fooled.

UCC-1: Expedia's where you got the flight from, right?

SOHAIB AKHTER: Yeah, got the flight, got the hotel, got the car, everything man.

UCC-1: Damn boy! We get flights, purchase flights and sell them.

SOHAIB AKHTER: Yeah, so Muneeb's trying to sell flights on the dark net. Inshallah, that may work, which is awesome.

21. On June 16, 2014, SOHAIB AKHTER posted on his Facebook profile page a picture of himself and MUNEEB AKHTER attending the 2014 TechConnect World Innovation Conference & Expo, in Prince George's County, Maryland. MUNEEB AKHER and SOHAIB AKHTER registered and paid for the Conference using identity theft victims' credit card information and means of identification.

22. On or about each of the dates set forth below, in the Eastern District of Virginia and elsewhere, MUNEEB AKHTER and 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

(All in violation of Title 18, United States Code, Section 1349)

COUNT TWO

(Conspiracy to Access a Protected Computer without Authorization)

THE GRAND JURY FURTHER CHARGES THAT:

23. The factual allegations in Paragraphs 1 through 22 are realleged and incorporated here.

24. Victim Company 1 housed a system of computers in its warehouse, in Sterling, Virginia, located in the Eastern District of Virginia.

25. Victim Company 1's system of computers was used in interstate and foreign commerce.

26. Victim Company 1's system of computers could only be accessed by authorized employees and agents of Victim Company 1.

27. Victim Company 1's system of computers processed records, including, but not limited to, credit card numbers and means of identification belonging to the identity theft victims.

28. Records pertaining to the identity theft victims' credit card numbers and means of identification could only be accessed by authorized employees and agents of Victim Company 1.

29. Each employee or agent who was authorized to access Victim Company 1's system of computers had a unique username and password that permitted access to the system. These usernames and passwords were designed to prevent unauthorized individuals from accessing the system.

30. Keystroke loggers were devices that could be installed on computers to record the identity and sequence of key strokes on a computer keyboard.

The Conspiracy

31. Between in or about March 2014, and continuing thereafter until in or about March 2015, in the Eastern District of Virginia and elsewhere, the defendants, MUNEEB AKHTER and SOHAIB AKHTER, knowingly and intentionally conspired and agreed together and with each other, and with others known and unknown to the Grand Jury, including UCC-1, 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 this Indictment, and the value of the information obtained exceeded $5,000, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i)-(iii).

MANNER AND MEANS OF THE CONSPRIACY

It was part of the conspiracy that:

32. 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.

33. 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.

34. Without the consent, authorization, or knowledge of Victim Company 1, its agents, or its employees, MUNEEB AKHTER would and did use the user name and password of at least one employee of Victim Company 1 to access Victim Company 1's system of computers.

35. MUNEEB AKHTER would and did use his access to the system to modify the website of Victim Company 1 by inserting computer codes. The codes caused the website to collect information from the online checkout page of the Company'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.

36. The computer code that MUNEEB AKHTER installed on Victim Company 1's website would and did cause the website to send emails containing the collected credit card

numbers and means of identification to email accounts controlled by MUNEEB AKHTER and SOHAIB AKHTER.

37. MUNEEB AKHTER and SOHAIB AKHTER and coconspirators would and did collect numerous credit card numbers and means of identification belonging to the identity theft victims.

38. MUNEEB AKHTER and SOHAIB AKHTER and coconspirators would and did use these numbers and means of identification to purchase goods and services throughout the United States.

OVERT ACTS

In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere:

39. In or about March 2014, in Sterling, Virginia, in the Eastern District of Virginia, MUNEEB AKHTER and SOHAIB AKHTER, UCC-1, and A.I. met in the warehouse of Victim Company 1. During the meeting, MUNEEB AKHTER and SOHAIB AKHTER stated a desire to hack websites in order to steal credit card information.

40. In or about April 2014, MUNEEB AKHTER and SOHAIB AKHTER created the following email accounts: credproc@hotmail.com and nsalookup@hotmail.com.

41. In or about April 2014, in Sterling, Virginia, in the Eastern District of Virginia, MUNEEB AKHTER entered Victim Company 1's warehouse without permission.

42. In or about April 2014, in Sterling, Virginia, in the Eastern District of Virginia, MUNEEB AKHTER used an employee's username and password that 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.

43. In or about April 2014, in Sterling, Virginia, in the Eastern District of Virginia, MUNEEB AKHTER installed a different computer code on Victim Company 1's website. The new code caused Victim Company 1's website to email the identity theft victims' information to nsalookup@hotmail.com.

44. On or about June 5, 2014, SOHAIB AKHTER and UCC-1 had the following conversation:

SOHAIB AKHTER: Muneeb said that he got 24 cc's today man.

UCC-1: Who said?

SOHAIB AKHTER: Muneeb.

UCC-1: From where?

SOHAIB AKHTER: 24 cc's from the site man.

UCC-1: From which site?

SOHAIB AKHTER: [Victim Company 1] man.

UCC-1: Seriously?

SOHAIB AKHTER: Yeah, 'cause it's emailing, it's . . . Muneeb put in the code so that, you know the FTP code that e-mails. He's getting the e-mails.

UCC-1: I thought they like reversed it already or something.

SOHAIB AKHTER: They may reverse the, like the website . . . yeah, the FTP goes a layer below, so it's already . . . it doesn't matter, it doesn't matter if you change the template back to the way it is. This is down low PHP man.

(All in violation of Title 18, United States Code, Section 371)

COUNTS THREE AND FOUR

(Aggravated Identity Theft)

THE GRAND JURY FURTHER CHARGES THAT

45. The factual allegations in Paragraphs 1 through 44 are realleged and incorporated here.

46. On or about the following instances, each instance constituting a separate count, in the Eastern District of Virginia and elsewhere, the defendant, MUNEEB AKHTER, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit conspiracy to commit wire fraud, as charged in Count One of this Indictment:

Count	Date	Person	Means of Identification
3	5/26/2014	D.F.	Name and address
4	5/26/2014	J.R.	Name and address

(All in violation of Title 18, United States Code, Sections 1028A(a)(2) and 2)

COUNTS FIVE AND SIX

(Aggravated Identity Theft)

THE GRAND JURY FURTHER CHARGES THAT

47. The factual allegations in Paragraphs 1 through 46 are realleged and incorporated here.

48. On or about the following instances, each instance constituting a separate count, in the Eastern District of Virginia and elsewhere, the defendant, SOHAIB AKHTER, did knowingly transfer, possess, and use, without lawful authority, a means of identification of

another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit conspiracy to commit wire fraud, as charged in Count One of this Indictment:

Count	Date	Person	Means of Identification
5	5/19/2014	A.H.	Name and address
6	5/16/2014	L.L.	Name and address

(All in violation of Title 18, United States Code, Sections 1028A(a)(2) and 2)

COUNT SEVEN

(Access of a Protected Computer without Authorization)

THE GRAND JURY FURTHER CHARGES THAT

49. The factual allegations in Paragraphs 1 through 48 are realleged and incorporated here.

50. Victim Company 2, known to the Grand Jury, is a company that aggregates data and information about federal government contracts and packages it in products used by federal government agencies and private contractors. It is located in Rockville, Maryland.

51. Victim Company 2's system of computers was used in interstate and foreign commerce.

52. In or about November 2013, A.M., the CEO of Victim Company 2, hired MUNEEB AKHTER and SOHAIB AKHTER as contractors to work on the Company's servers. The work was to be performed via the Internet, and did not require MUNEEB AKHTER and SOHAIB AKHTER to be physically present at Victim Company 2's offices.

53. In or about early November 2013, during a meeting with A.M., SOHAIB AKHTER and MUNEEB AKHTER told A.M. that they wanted access to the federal data stored

in Victim Company 2's database. A.M. informed the defendants that they would have to pay for a subscription if they wanted access to the data.

54. In an email sent from MUNEEB AKHTER to SOHAIB AKHTER, dated on or about November 27, 2014, MUNEEB AKHTER wrote that he "modified one of [A.M.'s] past logins to the front end.. it was really hard . . . ." MUNEEB AKHTER also indicated that he had created several new login accounts and passwords, which gave him additional "backend" access to Victim Company 2's computer systems.

55. MUNEEB AKHTER's hack of Victim Company 2 enabled MUNEEB AKHTER to access the entirety of Victim Company 2's systems, including the full range of Victim Company 2's federal data. MUNEEB AKHTER was not authorized to access Victim Company 2's computer systems in this manner, nor was he authorized to have access to the federal data.

56. On or about February 8, 2014, A.M. sent an email to MUNEEB AKHTER titled "Over 10,000 emails." A.M. wrote as follows:

> Muneeb,
>
> I believe you might have used the fedmine.us server again for emailing out something. I am getting 10 emails per second as undeliverable all to GMU addresses. . . . PLEASE TAKE THIS AS A SERIOUS MATTER AND SHUT DOWN THE NON DELIVERIES NOW.

MUNEEB AKHTER wrote the following email to A.M. in response:

> Dear [A.M.],
>
> I honestly regret what I have done. There was no reason to access your systems or place the code responsible for sending out spam to GMU emails nor was there reason to have your account host php scripts to offload cookie requests to voting servers. I misused your trust and system, and you did provide us with friendly treatment when we arrived at your house. . . . Aggression may leave us and our companies both in a bad position, so please, for a friend—do not go ahead with any legal actions/complaints. The authorities who may put me on trial will also revoke access to your data.

57. On or about November 27, 2013, and on or about February 8, 2014, within the Eastern District of Virginia and elsewhere, the defendant, MUNEEB AKHTER, intentionally accessed a computer without authorization and exceeded authorized access to a computer, and thereby obtained information from a protected computer, and the offense was committed for purposes of commercial advantage and private financial gain, and the value of the information obtained exceeded $5,000.

(All in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i), (iii))

COUNT EIGHT

(Conspiracy to Access a Government Computer without Authorization)

THE GRAND JURY FURTHER CHARGES THAT

58. The factual allegations in Paragraphs 1 through 57 are realleged and incorporated here.

59. The U.S. Department of State (hereinafter "State Department") is a department and agency within the executive branch of the U.S. Government. It has physical offices in Washington, DC.

60. The Bureau of Consular Affairs (hereinafter "Bureau") is a division of the State Department, which administers laws, formulates regulations, and implements policies relating to consular services and immigration. It has physical offices in Washington, DC.

61. Passport Lockbox (hereinafter "Lockbox") is 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, parent information, spouse's name, and emergency contact information.

62. ActioNet, Inc. (hereinafter "ActioNet") is a contractor that provided information technology support to the State Department. It has physical offices in Falls Church, Virginia, located in the Eastern District of Virginia.

63. From in or about October 2014 to in or about February 2015, SOHAIB AKHTER was a contract employee at ActioNet assigned to a position at the State Department as a Tier II Application Support Resource in the Data Engineering and Data Management Program within the Bureau.

64. 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.

65. 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.

66. 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."

67. 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.

The Conspiracy

68. Between in or about June 2014, and continuing thereafter until in or about March 2015, in the Eastern District of Virginia and elsewhere, the defendants, MUNEEB AKHTER and SOHAIB AKHTER, each knowingly and intentionally conspired and agreed together and with each other, and with others known and unknown to the Grand Jury, including UCC-1, 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, Section 1030(a)(2)(B) and (c)(2)(B)(i)-(iii).

MANNER AND MEANS OF THE CONSPIRACY

It was part of the conspiracy that:

69. MUNEEB AKHTER and SOHAIB AKHTER, UCC-1, and other coconspirators known and unknown to the Grand Jury, 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.

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

71. SOHAIB AKHTER also attempted to use his access to State Department computer systems to create an unauthorized account that would enable him to access State Department computer systems undetected. SOHAIB AKHTER surreptitiously installed malicious programs onto State Department computer systems in order to execute his plan to create the backdoor login account.

72. SOHAIB AKHTER orchestrated a scheme to secretly install a physical device at a State Department building known as SA-17. Once installed, the device would enable SOHAIB

AKHTER and coconspirators to collect data from and remotely access State Department computer systems.

73. 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.

74. 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 transmit it wirelessly to computers controlled by MUNEEB AKHTER and SOHAIB AKHTER and coconspirators.

75. On the day the scheme was executed, UCC-1 transported materials, including the gumstix, from MUNEEB AKHTER, located at the AKHTER residence, to SOHAIB AKHTER, located at SA-17.

OVERT ACTS

In furtherance of the conspiracy and to effect the objects of the conspiracy, the following overt acts, among others, were committed in the Eastern District of Virginia and elsewhere:

76. On or about June 24, 2014, MUNEEB AKHTER began working for defense contractor General Dynamics. He was hired to work as an Information Technology Security Specialist at DHS.

77. On or about June 24, 2014, MUNEEB AKHTER and SOHAIB AKHTER had the following conversation:

> 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. Know your shit. Need to know who's watching. 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.

78. In or about October 2014, SOHAIB AKHTER was hired by ActioNet to perform contract work for the State Department at both ActioNet offices in Falls Church, Virginia, and Bureau offices in Washington, DC.

79. 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, while employed at ActioNet, accessed the Lockbox database without authorization.

80. Between on or about February 12, 2015, and on or about February 19, 2015, SOHAIB AKHTER conducted approximately 119 searches for U.S. passport records using the Passport Lockbox Lookup report. He accessed personal passport information for approximately 62 different individuals, including: G.R., a DHS special agent investigating the crimes alleged in this Indictment; UCC-1; A.I.; A.M., the CEO of Victim Company 2; and himself. In addition, SOHAIB AKHTER attempted to access passport information for S.T., a DHS special agent investigating the crimes alleged in this Indictment.

81. 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.

82. In or about February 2015, SOHAIB AKHTER viewed and copied from State Department computer systems the personal passport information associated with several individuals, including DHS Special Agent G.R.

83. In or about March 2015, MUNEEB AKHTER told UCC-1 that he and SOHAIB AKHTER stored the personal passport information that SOHIAB AKHTER removed from State Department systems on an external hard drive. MUNEEB AKHTER told UCC-1 that Special

Agent G.R.'s information would be valuable to criminals on the "dark net" and that he was considering selling the information.

84. In or about February 2015, SOHAIB AKHTER downloaded several programs to a State Department computer. These programs included malicious software, or malware, which SOHAIB AKHTER hoped would enable him to access State Department computers remotely.

85. In or about February 2015, SOHAIB AKHTER told UCC-1 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 on the "dark net."

86. On or about February 15, 2015, SOHAIB AKHTER called UCC-1 and asked him to buy a drill. UCC-1 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 told UCC-1 that he was programming a SD card, which was later to be inserted into the gumstix. MUNEEB AKHTER gave UCC-1 a bag containing a screwdriver, tape, glue, and the gumstix. Pursuant to SOHAIB AKHTER's request, UCC-1 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 SD card to SOHAIB AKHTER.

87. 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.

88. On or about February 19, 2015, SOHAIB AKHTER sent an email from his State Department email account to the email address akhters3@vcu.edu containing lines of code and headers for State Department servers.

(All in violation of Title 18, United States Code, Section 371)

COUNT NINE

(False Statements)

THE GRAND JURY FURTHER CHARGES THAT

89. The factual allegations in Paragraphs 1 through 88 are realleged and incorporated here.

90. On or about June 26, 2014, the defendant, MUNEEB AKHTER, did willfully and knowingly make a materially false, fictitious, and fraudulent statement and representation in a matter within the jurisdiction of the executive branch of the Government of the United States, by telling a special agent of the U.S. Department of Homeland Security, in a written statement, that he had created a computer code that allowed him to add funds to gift cards produced by companies including K-Mart, Shell Gasoline, Whole Foods, Starbucks, and Dunkin Donuts without having to expend any actual funds. The statement and representation was false because, as defendant MUNEEB AKHTER then and there knew, the computer code did not exist and was simply a cover for his fraudulent use of stolen credit card numbers.

(All in violation of Title 18, United States Code, Section 1001(a)(2))

COUNT TEN

(False Statements)

THE GRAND JURY FURTHER CHARGES THAT

91. The factual allegations in Paragraphs 1 through 90 are realleged and incorporated here.

92. On or about October 17, 2014, the defendant, MUNEEB AKHTER, did willfully and knowingly make a materially false, fictitious, and fraudulent statement and representation in a matter within the jurisdiction of the executive branch of the Government of the United States, by answering several questions falsely on a Questionnaire for National Security Positions (hereinafter "e-QIP") administered by the U.S. Office of Personnel Management.

93. In or about October 2014, MUNEEB AKHTER obtained a position with defense contractor Booz-Allen Hamilton. After being hired, the defendant was required to complete an e-QIP.

94. A section of the e-QIP form includes the following questions specifically related to the "Use of Information Technology Systems":

a. In the last 7 years have you illegally or without proper authorization accessed or attempted to access any information technology system?

b. In the last 7 years, have you introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, guidelines, or regulations or attempted any of the above?

MUNEEB AKHTER falsely responded "No" to these questions.

95. These representations were false because, as MUNEEB AKHTER then and there knew, prior to completing the e-QIP, he had illegally and without proper authorization accessed computer systems belonging to Victim Company 1 and Victim Company 2. In addition, MUNEEB AKHTER had introduced unauthorized code and programs onto computer systems belonging to Victim Company 1 and Victim Company 2.

96. MUNEEB AKHTER falsely answered other questions on the e-QIP. Another section instructed him to list all places of employment for the prior 10 years. The defendant did not identify his prior employment with General Dynamics as part of his employment history.

97. Another section of the e-QIP asked MUNEEB AKHTER if he was ever fired from a job. The defendant falsely responded "No," despite knowing then and there that he had been fired from General Dynamics on July 2, 2014.

(All in violation of Title 18, United States Code, Section 1001(a)(2))

COUNT ELEVEN

(False Statements)

THE GRAND JURY FURTHER CHARGES THAT

98. The factual allegations in Paragraphs 1 through 97 are realleged and incorporated here.

99. On or about February 20, 2015, the defendant, SOHAIB AKHTER, did willfully and knowingly make a materially false, fictitious, and fraudulent statement and representation in a matter within the jurisdiction of the executive branch of the Government of the United States, by telling special agents of the U.S. Department of State, in a sworn statement, that he: (1) never modified or manipulated a computer system without authorization; and (2) never introduced hardware or software onto a computer system without authorization. The statement and representation was false because, as defendant SOHAIB AKHTER then and there knew, he and coconspirators illegally and without proper authorization modified and manipulated computer systems belonging to Victim Company 1 and the State Department and introduced unauthorized code and programs onto those systems.

(All in violation of Title 18, United States Code, Section 1001(a)(2))

COUNT TWELVE

(Obstruction of Due Administration of Justice)

THE GRAND JURY FURTHER CHARGES THAT

100. The factual allegations in Paragraphs 1 through 99 are realleged and incorporated here.

101. Defendant MUNEEB AKHTER was on release pursuant to an order dated March 2, 2015, from the United States District Court for the Eastern District of Virginia, Case No. 1:15MJ123, which order notified said defendant of the potential effect of committing an offense while on pretrial release.

102. While he was on release, beginning on or about March 2, 2015, and continuing through on or about April 30, 2015, the defendant, MUNEEB AKHTER, did corruptly influence, obstruct, and impede and endeavor to influence, obstruct, and impede, the due administration of justice in United States v. MUNEEB AKHTER and SOHAIB AKHTER, No. 1:15MJ123, in the United States District Court for the Eastern District of Virginia, by:

a. On or about March 20, 2015, asking UCC-1 to remove the code from Victim Company 1's website that was sending information to nsalookup@hotmail.com;

b. Encouraging UCC-1 to leave the United States in order to avoid federal investigators;

c. On or about March 24, 2015, sending the following message to A.I.: "Yo let [UCC-1] know that all he needs to do is not tlk to feds no matter what n wait a few months n we can win this n bcom instant millionaires";

d. On or about March 19, 2015, purchasing a flight for UCC-1 to travel from Washington, DC, to the Republic of Malta, which UCC-1 accepted and used that day to leave the United States;

e. Encouraging UCC-1 to travel to Saudi Arabia and stay there with MUNEEB AKHTER and SOHAIB AKHTER's father;

f. Encouraging UCC-1 to stay out of the United States until the investigation and prosecution in this case were concluded;

g. Upon UCC-1's return to the United States on or about March 31, 2015, encouraging UCC-1 to avoid federal agents investigating the case;

h. On or about April 1, 2015, sending the following message to UCC-1: "Nigga SOP is 2 months after one arrest they make the other.. stay outta DC area or anywhere theyd think to look..other than that you should be clear."

(All in violation Title 18, United States Code, Sections 1503 and 3147(1))

NOTICE OF FORFEITURE

Pursuant to Federal Rule of Criminal Procedure 32.2(a), each defendant is notified that, if convicted of any of the offenses alleged in Counts One, Two, Seven, and Eight above, he shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 1030(i), and Title 28, United States Code, Section 2461(c), the defendant's interest in any personal property that was used or intended to be used to commit or facilitate the commission of such violations, and any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violations.

If any of the property described above as being forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C); Title 28, United States Code, Section 2461(c); and Title 18, United States Code, Section 1030(i) as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

it is the intention of the United States of America, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c); and Title 18, United States Code, Section 1030(i)(2), to seek forfeiture of substitute assets.

(All pursuant to 18 U.S.C. §§ 981(a)(1)(C) and 1030(i), and 28 U.S.C. § 2461(c); Rule 32.2(a), Federal Rules of Criminal Procedure)

A TRUE BILL:

Foreperson of the Grand Jury

DANA J. BOENTE
UNITED STATES ATTORNEY

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

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