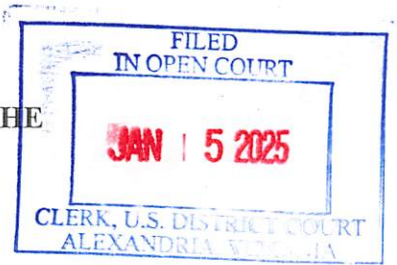


IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division



UNITED STATES OF AMERICA

v.

MUNEEB AKHTER
a/k/a MICKEY AKHTER
a/k/a MUNIB AKHTER
(Counts 1-6 and 9-12)
and

SOHAIB AKHTER
a/k/a SUHAIB AKHTER,
(Counts 1, 7-8, and 13)

Defendants.

Case No. 1:25-CR-307

Count 1: Conspiracy (18 U.S.C. § 371)

Count 2: Intentional Damage to a Protected
Computer Without Authorization
(18 U.S.C. §§ 1030(a)(5) and
(c)(4)(C)(i))

Count 3: Obtaining Information from
Computer Without Authorization
(18 U.S.C. §§ 1030(a)(2) and
(c)(2)(C), 2)

Count 4: Theft of United States Government
Records (18 U.S.C. § 641)

Counts 5-6: Aggravated Identity Theft
(18 U.S.C. § 1028A(a)(1))

Count 7: Password Trafficking
(18 U.S.C. § 1030(a)(6))

Count 8: Possession of a Firearm by a
Prohibited Person (18 U.S.C.
§ 922(g)(1))

Counts 9-10: Wire Fraud (18 U.S.C. §§ 1343 and
2)

Count 11: Aggravated Identity Theft
(18 U.S.C. § 1028A(a)(1))

Count 12: Possession of 15 or More
Unauthorized Access Devices
(18 U.S.C. § 1029(a)(3))

Count 13: Witness Tampering
(18 U.S.C. § 1512(b)(1))

Forfeiture Notice

SUPERSEDING INDICTMENT

January Term - at Alexandria, Virginia

COUNT ONE

(Conspiracy to Commit Computer Fraud and to Destroy Records)

THE GRAND JURY CHARGES THAT:

1. Beginning at a time unknown to the Grand Jury but no later than February 18, 2025, and continuing through at least February 25, 2025, the defendants, **MUNEEB AKHTER** and **SOHAIB AKHTER**, conspired and agreed to steal and destroy government information. Following their termination from a government contractor (Company-1), the Defendants sought to harm the company and numerous federal government agencies by deleting databases, stealing information, and destroying evidence of their unlawful activities.

General Allegations

At times material to this Indictment:

2. Defendant **MUNEEB AKHTER**, who also went by **MICKEY AKHTER** and **MUNIB AKHTER**, resided in the Eastern District of Virginia until on or about February 24, 2025. After on or about February 24, 2025, he temporarily resided in the Northern District of Texas, and then in the District of Utah, and made multiple trips back to the Eastern District of Virginia. Defendant **MUNEEB AKHTER** had previously been convicted of Access of a Protected Computer Without Authorization, in violation of Title 18, United States Code, Section 1030(a)(2)(C) and (c)(2)(B)(i), (iii), among other offenses, on June 26, 2015 in the United States District Court for the Eastern District of Virginia.

3. Defendant **SOHAIB AKHTER**, who also went by **SUHAIB AKHTER**, resided in the Eastern District of Virginia.

4. **MUNEEB AKHTER** was employed by Company-1 from on or about October 2, 2023, to February 18, 2025. **SOHAIB AKHTER** was employed by Company-1 from on or about March 27, 2024, to February 18, 2025.

5. Company-1 was a company headquartered in Washington, D.C. Company-1 provided software products and services to more than forty-five United States federal government agencies. Company-1 hosted data for some federal government clients on servers located in Ashburn, Virginia. Other federal government clients used Company-1's software but hosted their data on their own servers.

6. The United States Equal Employment Opportunity Commission (EEOC) was a federal agency located in Washington, D.C. The EEOC was a customer of Company-1 and hosted data on Company-1's servers.

7. The United States Department of Homeland Security (DHS) was a federal agency located in Washington, D.C. The DHS was a customer of Company-1 and hosted data on Company-1's servers.

8. The United States Internal Revenue Service (IRS) was a federal agency located in Washington D.C. The IRS was a customer of Company-1 and hosted data on Company-1's servers.

The Conspiracy

9. From at least on or about February 18, 2025, to at least on or about February 25, 2025, within the Eastern District of Virginia, the Defendants, **MUNEEB AKHTER** and **SOHAIB AKHTER**, did knowingly and unlawfully conspire to commit and to aid and abet the following offenses against the United States:

- a. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without

authorization to a protected computer; such damage causing the loss to one or more persons during any one-year period, and loss resulting from a related course of conduct affecting one or more other protected computers, aggregating at least \$5,000 in value; and affecting a computer used by and for an entity of the United States Government in furtherance of the administration of justice, national defense, and national security; and cause damage affecting 10 or more protected computers during a one-year period, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(B), and 1030(c)(4)(A)(i)(I),(V)-(VI), 2;

b. to knowingly alter, destroy, mutilate, conceal, cover up, falsify, and make a false entry in a record, document, and tangible object with the intent to impede, obstruct, and influence the investigation and proper administration of a matter within the jurisdiction of a department and agency of the United States and a case filed under title 11, and in relation to and contemplation of such matter and case, in violation of Title 18, United States Code, Sections 1519, 2.

Manner and Means of the Conspiracy

10. Following their termination from Company-1 on February 18, 2025, **MUNEEB AKHTER** and **SOHAIB AKHTER** sought to harm Company-1 and its U.S. government customers by accessing computers without authorization, write-protecting databases, deleting databases, stealing information, and destroying evidence of their unlawful activities. When the Defendants did not know the database commands necessary to accomplish their unlawful objectives, they used an artificial intelligence tool to help them. After deleting databases and event logs, the Defendants later used anti-forensic techniques, reinstalled the operating systems on the Company-1 laptops to which they had been previously assigned, and concealed evidence, in attempts to prevent the analysis of the Company-1 laptops and hamper the investigation into their criminal activities.

Overt Acts

11. In furtherance of the conspiracy, and to effect the objects thereof, the defendants and others, both known and unknown to the Grand Jury, committed, and caused to be committed, the following acts, among others, in the Eastern District of Virginia and elsewhere:

12. On February 18, 2025, at approximately 4:55 p.m. and approximately five minutes after being fired by Company-1, **SOHAIB AKHTER** unsuccessfully attempted to access Company-1's computer network without authorization. **SOHAIB AKHTER** failed to do so because his virtual private network connection had been deactivated, and his Windows account had been disabled at approximately 4:50 p.m.

13. On February 18, 2025, at approximately 4:55 p.m. and approximately five minutes after being fired by Company-1, **MUNEEB AKHTER** accessed Company-1's computer network without authorization and told **SOHAIB AKHTER** he was still connected to the network.

14. On February 18, 2025, at approximately 4:56 p.m., **MUNEEB AKHTER** accessed a government agency's database on a Company-1 server, issued commands to prevent other users from connecting or making changes to the database, and then issued a command to delete the database.

15. On February 18, 2025, between approximately 4:56 p.m. and 5:52 p.m., **MUNEEB AKHTER** deleted approximately 96 databases storing U.S. government information that were hosted by Company-1. Many of these databases contained records and documents related to Freedom of Information Act matters administered by federal government departments and agencies, as well as sensitive investigative files of federal government departments and agencies.

16. On February 18, 2025, at approximately 4:58 p.m., **MUNEEB AKHTER** issued commands that deleted a DHS production database containing U.S. government information. The database was hosted on a Company-1 server in the Eastern District of Virginia.

17. On February 18, 2025, at approximately 4:59 p.m., **MUNEEB AKHTER** asked an artificial intelligence tool, “how do i clear system logs from SQL servers after deleting databases.”

18. On February 18, 2025, at approximately 5:14 p.m., **SOHAIB AKHTER** stated aloud, “They’re gonna probably raid this place,” to which **MUNEEB AKHTER** replied, “I’ll clean this shit up.” **SOHAIB AKHTER** responded, “We also gotta clean stuff up from the other house, man.”

19. On February 18, 2025, at approximately 5:44 p.m., **MUNEEB AKHTER** asked artificial intelligence tool, “how do you clear all event and application logs from Microsoft windows server 2012.”

20. On February 18, 2025, at approximately 6:22 p.m., **MUNEEB AKHTER** attached a USB drive to a Company-1-owned laptop which had been previously assigned to him.

21. On February 18, 2025, between approximately 6:22 p.m. and 6:28 p.m., **MUNEEB AKHTER** copied approximately 1,805 files belonging to the EEOC from the Company-1-owned laptop to the USB drive.

22. On February 18, 2025, at approximately 6:31 p.m., **MUNEEB AKHTER** removed the USB drive from the Company-1-owned laptop.

23. On February 18, 2025, at approximately 11:16 p.m., **MUNEEB AKHTER** created an archive file called “source.7z,” using the Company-1-owned laptop to which he was previously assigned.

24. On February 20, 2025, between approximately 8:51 p.m. and 8:59 p.m., **MUNEEB AKHTER** attempted to access a DHS-owned laptop without authorization at least three times.

25. On or about February 21, 2025, a co-conspirator wiped the contents of **MUNEEB AKHTER's** Company-1-issued laptop by re-installing the operating system.

26. On or about February 21, 2025, a co-conspirator wiped the contents of **SOHAIB AKHTER's** Company-1-issued laptop by re-installing the operating system.

27. On February 24, 2025, **MUNEEB AKHTER** drove to Texas. He transported his personal laptop, mobile device, and a Personal Identify Verification (PIV) card issued by a U.S. government agency.

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

COUNT TWO
(Intentional Damage to a Protected Computer)

THE GRAND JURY FURTHER CHARGES THAT:

28. The allegations set forth in paragraphs 2 through 8 and 10 through 27 are realleged and incorporated as if fully set forth herein.

29. On or about February 18, 2025, in the Eastern District of Virginia and elsewhere, the defendant, **MUNEEB AKHTER**, knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, that is, a computer owned by Company-1 that hosted a database containing information belonging to the Department of Homeland Security, such offense occurring after a conviction for another offense under 18 U.S.C. § 1030.

(In violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(C)(i).)

COUNT THREE

(Obtaining Information from a Computer Without Authorization)

THE GRAND JURY FURTHER CHARGES THAT:

30. The allegations set forth in paragraphs 2 through 8 and 10 through 27 are realleged and incorporated as if fully set forth herein.

31. On or about February 18, 2025, in the Eastern District of Virginia and elsewhere, the defendant, **MUNEEB AKHTER**, did intentionally access a computer without authorization and thereby obtained information from a department and agency of the United States, that is, the EEOC, and from a protected computer, that is, a Company-1 computer hosting EEOC information, aiding and abetting the same, such offense occurring after a conviction for another offense under 18 U.S.C. § 1030.

(In violation of Title 18, United States Code, Sections 1030(a)(2)(B), (a)(2)(C), (c)(2)(C) and 2.)

COUNT FOUR
(Theft of Government Records)

THE GRAND JURY FURTHER CHARGES THAT:

32. The allegations set forth in paragraphs 2 through 8 and 10 through 27 are realleged and incorporated as if fully set forth herein.

33. From at least in and around February 2025 through on or about March 12, 2025, within the Eastern District of Virginia and elsewhere, the defendant, **MUNEEB AKHTER**, did willfully and knowingly steal, purloin, and convert to his use and the use of another, any record and thing of value of the United States and of any department or agency thereof, to wit: copies of IRS information stored on a virtual machine, including (1) copies of federal tax information and other identifying information of at least 450 individuals, (2) copies of at least 100 reports containing confidential IRS data related to analysis of and weaknesses in other agencies' safeguards for federal tax information, and (3) copies of hundreds of Freedom of Information Act requests, the value of such property in the aggregate exceeding \$1,000.

(In violation of Title 18, United States Code, Section 641.)

COUNT FIVE
(Aggravated Identity Theft)

THE GRAND JURY FURTHER CHARGES THAT:

34. The allegations set forth in paragraphs 2 through 8 and 10 through 27 are realleged and incorporated as if fully set forth herein.

35. From at least in or around February 2025 to on or about March 12, 2025, within 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 a real person, specifically, a Social Security number belonging to Victim-1 included in IRS information stored by Company-1, during and in relation to the specified violation of Title 18, United States Code, Section 641, that is charged in Count Four.

(In violation of Title 18, United States Code, Section 1028A(a)(1).)

COUNT SIX
(Aggravated Identity Theft)

THE GRAND JURY FURTHER CHARGES THAT:

36. The allegations set forth in paragraph 2 are realleged and incorporated as if fully set forth herein.

37. On or about August 15, 2022, in the Eastern District of Virginia, defendant **MUNEEB AKHTER** knowingly possessed and used, without lawful authority, a means of identification of another actual person, including but not limited to the name, date of birth, Social Security number, and passport of Victim-2, during and in relation to a felony enumerated in Title 18, United States Code, Section 1028A(c), to wit, Misuse of a Passport, in violation of Title 18, United States Code, Section 1544.

(In violation of Title 18, United States Code, Section 1028A(a)(1).)

COUNT SEVEN

(Computer Fraud and Abuse – Password Trafficking)

THE GRAND JURY FURTHER CHARGES THAT:

38. The allegations set forth in paragraphs 2 through 8 are realleged and incorporated as if fully set forth herein.

39. On or about February 1, 2025, within the Eastern District of Virginia and elsewhere, the defendant, **SOHAIB AKHTER**, knowingly and with intent to defraud trafficked in a password and similar information through which a computer may be accessed without authorization, affecting interstate and foreign commerce, and such computer was used by and for the Government of the United States, specifically, a password providing access to a Company-1 computer used by the United States EEOC and to an email account owned by Victim-3.

(In violation of Title 18, United States Code, Section 1030(a)(6) and (c)(2)(A).)

COUNT EIGHT

(Possession of a Firearm by a Prohibited Person (18 U.S.C. § 922(g)(1))

THE GRAND JURY FURTHER CHARGES THAT:

40. The allegations set forth in paragraph 3 are realleged and incorporated as if fully set forth herein.

41. On or about March 12, 2025, a federal search warrant was executed at **SOHAIB AKHTER's** residence in Alexandria. Approximately 378 .30 caliber rounds of ammunition, located in an ammunition box, were found in a shed affixed to the residence.

42. On or about March 16, 2025, in the Eastern District of Virginia, the defendant, **SOHAIB AKHTER**, knowing that he had been convicted of crimes punishable by imprisonment for a term exceeding one year, specifically, Conspiracy to Commit Wire Fraud, Conspiracy to Access a Protected Computer without Authorization, and Conspiracy to Access a Government Computer Without Authorization, in the United States District Court for the Eastern District of Virginia, in case number 1:15-CR-124-TSE, did knowingly possess seven firearms, that is, a Springfield Armory, U.S. M1A rifle, serial number 047785; an H&R Arms Co., U.S. M1 rifle, serial number 4780522; a Marlin Firearms Co., Glenfield Model 60 semi-automatic rifle, serial number 26258114; a J.C. Higgins, Model 42, .22 caliber rifle, serial number 103,19800; a Ruger .22 caliber long range automatic pistol, serial number 7083; a Colt Police .38 caliber Special revolver, serial number 733585; and a Colt "The Woodsman" .22 caliber automatic pistol, serial number 111599, said firearms and ammunition having been shipped and transported in interstate and foreign commerce.

(In violation of Title 18, United States Code, Section 922(g)(1) and 924(a)(8).)

COUNTS NINE AND TEN
(Wire Fraud)

THE GRAND JURY FURTHER CHARGES THAT:

43. The allegations set forth in paragraphs 2 through 6 are realleged and incorporated as if fully set forth herein.

44. Beginning on a date unknown, but at least as early as in and around May 2025, and continuing through December 3, 2025, in the Eastern District of Virginia and elsewhere, the defendant **MUNEEB AKHTER**, did knowingly and with the intent to defraud, having devised and intending to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, transmit and caused to be transmitted, by means of wire communications in interstate and foreign commerce, writings, signs, signals, and sounds for the purpose of executing such scheme and artifice.

Purpose of the Scheme to Defraud

45. The purpose of the scheme to defraud was for the defendant to (1) steal valid usernames and passwords for the EEOC Public Portal, a web application developed and maintained by Company-1; (2) fraudulently use these stolen credentials without authorization to attempt to access and access email and other online accounts of victims using the stolen credentials (i.e., accounts that used the same password for web applications other than the EEOC Public Portal); (3) unlawfully use information obtained from the victims' various online accounts for their own personal benefit; and (4) conceal the scheme.

Manner and Means Used to Accomplish the Scheme to Defraud

46. The manner and means by which the defendant sought to accomplish the scheme included, among others, the following:

47. **MUNEEB AKHTER** transferred approximately 5,400 usernames (email addresses) and passwords from the Company-1 network, including the email address and password of Victim-3, as alleged in Count Seven, to computers he controlled. He stored copies of the stolen usernames and passwords on his personal laptop, on his personal Android phone, on an external hard drive, and in another cloud account he controlled.

48. **MUNEEB AKHTER** used the list of usernames and passwords to attempt to log into various websites where the victims may have accounts. In hundreds of instances, he successfully logged in to victims' email accounts without authorization.

49. **MUNEEB AKHTER** created and used Python scripts to test these credentials against the website of Company-2, a U.S.-based hotel chain.

50. Without authorization, **MUNEEB AKHTER** logged in to online airline, hotel, and bank accounts belonging to victims, in order to enrich himself. For example, between in or around April 2025 and December 3, 2025, **MUNEEB AKHTER** accessed or attempted to access victims' accounts with the following companies:

- a. Company-2, Company-3, and Company-4, U.S.-based hotel chains, and Company-5, a UK-based hotel chain.
- b. Company-6, Company-7, Company-8, and Company-9, all U.S.-based airlines.
- c. Company-10, Company-11, Company-12, Company-13, Company-14, Company-15, Company-16, and Company-17, all U.S.-based financial institutions.

51. In multiple instances, after successfully logging into a victim's airline, hotel, financial, or other online account without authorization, **MUNEEB AKHTER** changed the email address associated with the online account to a new email address created by **MUNEEB AKHTER**, such as "[Victim Name]@wardensys.com," which appeared to belong to the victim.

He created multiple email accounts designed to appear to belong to victims using wardensys.com and wardensystems.com, domains he controlled.

Wires in Interstate and Foreign Commerce

52. On or about the dates set forth below, within the Eastern District of Virginia and elsewhere, **MUNEEB AKHTER**, for the purpose of executing the scheme described above, caused to be transmitted, and aided and abetted the transmission of, by means of wire communication in interstate commerce, the writings, signs, signals, pictures, and sounds described below for each count, with each transmission constituting a separate count:

Count	Approximate Date (On or About)	Description
9	December 1, 2025	Company-6 online ticket booking made using Victim-4's airline miles from the Eastern District of Virginia, causing the transmission of an airline ticket confirmation code to the District of Massachusetts.
10	December 1, 2025	Attempt to log in to Victim-5's Company-18 account from the Eastern District of Virginia, causing the transmission of a two-factor authentication code to the District of Oregon.

(In violation of Title 18, United States Code, Section 1343 and 2.)

COUNT ELEVEN
(Aggravated Identity Theft)

THE GRAND JURY FURTHER CHARGES THAT:

53. The allegations set forth in paragraphs 2 through 6 and 45 through 51 are realleged and incorporated as if fully set forth herein.

54. On or about December 1, 2025, within the Eastern District of Virginia, the defendant, **MUNEEB AKHTER**, did knowingly transfer, possess, and use, without lawful authority, a means of identification of a real person, specifically, an email address, password, phone number, mailing address, and Company-6 rewards number, belonging to Victim-5, during and in relation to the specified violations of Title 18, United States Code, Section 1343, that are charged in Counts Nine and Ten.

(In violation of Title 18, United States Code, Section 1028A(a)(1).)

COUNT TWELVE

(Possession of 15 or More Unauthorized Access Devices)

THE GRAND JURY FURTHER CHARGES THAT:

55. The allegations set forth in paragraphs 2 through 6 and 45 through 51 are realleged and incorporated as if fully set forth herein.

56. On or about December 3, 2025, in the Eastern District of Virginia, the defendant, **MUNEEB AKHTER**, knowingly and with intent to defraud, possessed fifteen or more unauthorized access devices, that is, usernames and passwords capable of providing account access, without the authorization of the issuer of said access devices, affecting interstate and foreign commerce.

(In violation of Title 18, United States Code, Section 1029(a)(3).)

COUNT THIRTEEN
(Witness Tampering)

THE GRAND JURY FURTHER CHARGES THAT:

57. The allegations set forth in paragraphs 41 and 42 are realleged and incorporated as if fully set forth herein.

58. On or about December 18, 2025, in the Eastern District of Virginia, the defendant, **SOHAIB AKHTER**, did knowingly attempt to use intimidation, threaten, and corruptly persuade Person 1 by instructing Person 1 to convey false information regarding his procurement, possession, and sale of firearms, with the intent to influence the testimony of Person 1 in an official proceeding, namely, the Grand Jury's investigation into the conduct charged in Count Eight of this Indictment.

(In violation of Title 18, United States Code, Section 1512(b)(1).)

NOTICE OF FORFEITURE

THE GRAND JURY FURTHER FINDS PROBABLE CAUSE THAT:

The defendants, **MUNEEB AKHTER** and **SOHAIB AKHTER**, are hereby notified, pursuant to Federal Rule of Criminal Procedure 32.2(a), that upon conviction of any of the offenses alleged in Counts One through Thirteen of this Indictment, they shall forfeit to the United States, pursuant to, pursuant to pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i): (1) any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of the violation; and (2) any personal property used or intended to be used to commit or to facilitate the commission of the violation.

The defendant, **MUNEEB AKHTER**, is hereby notified, pursuant to Federal Rule of Criminal Procedure 32.2(a), that upon conviction of the offense alleged in Count Four of this Indictment, the defendant, **MUNEEB AKHTER**, shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. 18 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the violation.

The property subject to forfeiture includes, but is not limited to, the following:

1. MSI laptop (hard drive S/N FN08N830910908V14);
2. Apple iPhone XR (S/N F17YFAC9KXKN);
3. Apple iPhone XR (S/N F2LY8B02KXKP);
4. Google Android phone (IMEI 355984760425344);
5. Samsung cell phone 322 (IMEI 358533130160565);
6. Apple iPhone 15 Pro Max (S/N FLYV0N0VY1);
7. MSI laptop (S/N K2102N0020599);
8. MSI laptop (hard drive S/N S7M4NS0X119301H);

9. Motorola cell phone (IMEI 356125208073580);
10. Toshiba external drive (S/N F25311090903202);
11. Toshiba external drive (S/N 75SDTI90TCVJ); and
12. Avolusion external drive AVF332312000840.

If any property subject to forfeiture is unavailable, the United States may seek an order forfeiting substitute assets pursuant to Title 21, U.S. Code, Section 853(p) and Federal Rule of Criminal Procedure 32.2(e).

(Pursuant to 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2) and 1030(i); 21 U.S.C. § 853; 28 U.S.C. § 2461(c); and Fed. R. Crim. P. 32.2.)

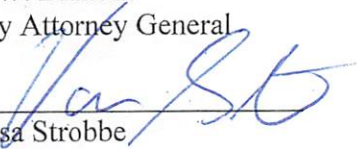
A TRUE BILL:

**Pursuant to the E-Government Act,
The original of this page has been filed
under seal in the Clerk's Office**

Foreperson of the Grand Jury

Lindsey Halligan
United States Attorney and Special Attorney

Todd W. Blanche
Deputy Attorney General


Vanessa Strobbe
Assistant United States Attorney

A. TYSEN DUVA
ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION


George S. Brown
Stefanie A. Schwartz
Trial Attorneys
U.S. Department of Justice, Criminal Division
Computer Crime and Intellectual Property Section