UNDER SEAL

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF NORTH CAROLINA
STATESVILLE DIVISION

UNITED STATES OF AMERICA,)	DOCKET NO. 5:16CR29-RLV
)	
v.)	BILL OF INDICTMENT
)	
)	
)	18 U.S.C. § 1343
)	18 U.S.C. § 1344
ALEKSANDR MUSIENKO,)	18 U.S.C. § 1956(h)
a/k/a "Oleksandr Serhiyovych Musiyenko")	18 U.S.C. § 1956(a)(2)(B)(i)
a/k/a "Robert Davis")	18 U.S.C. § 2
a/k/a "Ply")	
Defendant.)	
)	

THE GRAND JURY CHARGES:

At all times relevant to this Indictment:

INTRODUCTION

1. From at least in or about October 2009, through in or about March 2012, in Catawba County and Mecklenburg County, within the Western District of North Carolina, and elsewhere, the defendant ALEKSANDR MUSIENKO, a/k/a "Oleksandr Serhiyovych Musiyenko," a/k/a "Robert Davis," a/k/a "Ply," and other persons known and unknown to the Grand Jury, engaged in wire fraud, bank fraud, money laundering conspiracy, and money laundering through "money mule" services provided to cybercriminals.

2. MUSIENKO had a network of "money mules" throughout the United States with corporate and individual bank accounts that could be used to both assist cybercriminals in carrying out fraud schemes against victims in the United States, and to launder the proceeds of those frauds.

3. As charged in this Indictment, MUSIENKO partnered with certain cybercriminals to complete "Bank Account Takeover" wire fraud and bank fraud schemes.

a. These cybercriminals hacked and stole information from victims in the United States which could be used to impersonate the victims in order to, under fraudulent pretenses, "take over" the victims' bank accounts.

b. By tricking the victims' banks into believing that withdrawals from the victims' accounts were actually requested by the victims, the cybercriminals had the ability to steal large amounts of money from the victims' accounts that were "taken over."

c. MUSIENKO's money mule services completed the fraud by providing information about the money mules' bank accounts into which the victims' banks could be tricked into sending the victims' money.

4. Once the fraud was complete, MUSIENKO then provided money mule services to launder the funds. MUSIENKO would direct his money mules to launder the proceeds to overseas recipients.

5. Ultimately, from in or about October 2009 through in or about March 2012, MUSIENKO's criminal money mule services resulted in the theft and laundering of at least $2.8 million.

ENTITIES AND INDIVIDUALS

6. ALEKSANDR MUSIENKO ("MUSIENKO") was a Ukrainian national who resided in Ukraine. MUSIENKO, who also used the alias names "Robert Davis" and "Ply," was primarily responsible for recruiting, supervising and directing a network of "money mules" used to illegally launder funds stolen in the fraud schemes.

7. "Victim VDC" was a North Carolina corporation engaged in the business of manufacturing and distributing paper products. Victim VDC maintained its corporate office in Hickory, North Carolina, and operated five production facilities throughout the United States. Victim VDC maintained a commercial bank account at Bank #1 in connection with its business operations, and used computers in Hickory, North Carolina, to conduct online banking transactions.

8. "Other Victims" were businesses and individuals located throughout the United States who maintained commercial and personal bank accounts respectively at various banks throughout the United States in connection with their business operations and personal finances respectively. The Other Victims used their computers to conduct online banking transactions.

9. Bank #1 was a financial institution with branch offices located within the Western District of North Carolina and elsewhere, the accounts and deposits of which were insured by the Federal Deposit Insurance Corporation ("FDIC"). Bank #1 maintained the commercial bank account of Victim VDC.

10. Western Union was a money transfer company whose activities affected interstate and foreign commerce. Western Union had offices located throughout the United States, and transferred funds throughout the world by wire transfers that were electronically routed to and processed in Western Union facilities located in Charlotte, Mecklenburg County, North Carolina.

DEFINITIONS

11. As used in this Indictment,

a. "malware" was malicious software designed to execute multiple unauthorized operations on malware-infected computers, including the theft of online banking credentials and control of victims' computers to fraudulently execute unauthorized banking transactions by wire.

b. "money mules" were people who were used to transfer and launder stolen funds. Money mules were either aware ("witting") or unaware ("unwitting") that they were being used to assist in the execution of the wire fraud and bank fraud scheme and then to launder the proceeds of those schemes overseas.

c. "money-mule bank accounts" were bank accounts owned and controlled by money mules, and were used to receive funds obtained by wire fraud and bank fraud and then launder the proceeds of the schemes outside the United States, either directly from the money mule accounts by wire, or through cash withdrawals and subsequent wire transfers through Western Union.

12. A "bank account takeover" scheme is a scheme and artifice to defraud and to obtain money and property of a victim, and to obtain funds under the custody and control of financial institutions that involved wire communications to:

a. secretly install hidden malicious software ("malware") on computers of the victim.

b. use the installed malware to steal online banking log-in credentials from the malware-infected computers of the victim.

c. use the stolen online banking credentials and computers of the victim to pose as the victim, trick the bank under fraudulent pretenses into believing that the victim was requesting a withdrawal or transfer, and make fraudulent unauthorized wire transfers of funds out of the bank accounts of the victim into bank accounts of "money mules."

MUSIENKO'S MONEY MULE SERVICES FOR CYBERCRIMINALS

ESTABLISHING THE INFRASTRUCTURE

13. In or about April 2007, MUSIENKO subscribed for one or more "Hotmail" e-mail accounts with Microsoft, Inc., which provides e-mail services to users around the world. These included "uif-service@hotmail.com." MUSIENKO used this account to receive "employment agreements" from the "money mules," voicemail messages from people inquiring about the supposed "financial assistant" employment positions which were in reality money mule positions, and written wire transfer confirmations from his money mules' banks, which had been forwarded by his money mules.

14. In or about September 2009, MUSIENKO subscribed for an account with J2 Communications, which provides linked facsimile, e-mail, and other communications services, and he connected the facsimile number to his uif-service@hotmail.com e-mail account.

15. In or about November 2010, MUSIENKO registered the domain name "imes-mgmt.com" with a domain name registrar.

16. In or about September 2011, MUSIENKO registered the domain name "vita-financial.com" with a domain name registrar. He created various e-mail accounts associated with that domain name, including info@vita-financial.com.

17. In or about September 2011, MUSIENKO subscribed for an account with Skype, which provides voice-over-internet protocol telephone communication services.

18. In or about September 2011, MUSIENKO created a phony company called "Vita Finance AG," or "Vita Financial AG," which he used to recruit and task money mules.

19. In or about September 2011, MUSIENKO subscribed for one or more "Gmail" e-mail accounts with Google, Inc., which provided e-mail services to users around the world. These included "vitafinancialinc@gmail.com."

20. On or about December 2011, MUSIENKO created a phony company called "Hilpert AG," which he used to recruit and task money mules.

CREATING THE MONEY MULE NETWORK

21. MUSIENKO, using aliases that included "Robert Davis" and phony front companies that included "Vita Finance AG" and "Hilpert AG," recruited money mules throughout the United States using a variety of techniques, including by advertising bogus "employment" opportunities to work as "Financial Assistants." MUSIENKO promised to pay the money mules a fee of approximately 5% for each overseas wire transfer they completed.

22. For example, on or about September 2011, MUSIENKO created an e-mail solicitation seeking to hire "Financial Assistants," purporting to be sent from "Robert Davis" from a company called "Vita Financial AG." In the solicitation, MUSIENKO explained that Vita Finance "perform[s] financial services for our clients and partners" to protect them from problems with "double taxation" due to "different tax systems in USA and Europe." MUSIENKO explained that the Financial Assistant would receive bank transfers from Vita Finance's "clients" into the Financial Assistant's personal or corporate/business account and then would transfer those funds to another designated bank account. MUSIENKO offered to pay the Financial Assistant 5% of the transaction amount. He stated that "we can guarantee 2-3 transfers per week, for amounts approx $30,000 weekly inflow to personal account, and approx $100,000 to corporate account." MUSIENKO repeatedly stated that the "financial services" that Vita Finance AG provided were "100% legal" and that "we perform our financial services 100% legally, following all international laws and rules." He included an employment "application," which

consisted of a list of questions seeking personally identifiable information and bank account information. He also directed prospective employees to visit the website identified by the domain name www.vita-financial.com to obtain more information

23. On or about September 12, 2011, MUSIENKO, posing as "Robert Davis" with "Vita Finance AG," communicated with J.H. by e-mail regarding employment as a "USA Financial Assistant" for Vita Finance AG. MUSIENKO sent J.H. an e-mail solicitation, which is described above. MUSIENKO promised to pay J.H. 5% of every transaction amount that she transferred. MUSIENKO then asked J.H. to provide him with J.H.'s bank account information.

24. On or about September 12, 2011, MUSIENKO, posing as "Robert Davis" with "Vita Finance AG," communicated with B.S. by e-mail and by phone regarding employment as an Account Manager or Sales Manager for Vita Finance AG. MUSIENKO explained to B.S. that Vita Finance's clients were businesses that hired Vita Finance to assist them in transferring funds out of the United States. MUSIENKO then asked B.S. to provide the bank account information that he would be using for his "job." MUSIENKO promised to pay B.S. approximately 5% of every transaction amount that he transferred.

25. In or about December 2011, MUSIENKO posted an online advertisement on the online employment website "monster.com," advertising a similar employment position with "Hilpert AG."

26. On or before December 20, 2011, MUSIENKO, posing as "Robert Davis" with "Hilpert AG," communicated with K.R. by e-mail and by phone regarding employment with Hilpert AG. MUSIENKO explained to K.R. that K.R. would receive bank transfers from Hilpert's "clients" into K.R.'s personal or corporate/business account. K.R. would then withdraw those funds in cash, take the cash to the nearest Western Union location, and wire the funds from Western Union in designated amounts, to designated individuals, at designated overseas cities and countries. K.R. would then obtain from Western Union a Money Transfer Control Number ("MTCN"), a 10-digit tracking number that Western Union generates for each transfer, and forward that MTCN number to MUSIENKO. MUSIENKO offered to pay K.R. approximately 5% of the transaction amount. MUSIENKO then asked K.R. to provide him with K.R.'s bank account information.

27. Using these and other methods, MUSIENKO recruited dozens of witting and unwitting U.S.-based money mules. MUSIENKO's money mules included:

a. J.H., an individual who resided in California and had accepted MUSIENKO's fake employment offer to be a "Financial Assistant" with "Vita Finance" in or about September 2011. J.H. had access to a corporate bank account held at J.P. Morgan Chase Bank NA ("J.P. Morgan"), a federally-insured financial institution.

b. B.S., an individual who resided in Idaho and had accepted MUSIENKO's fake employment offer to be an "Account Manager" or "Sales Manager with "Vita Finance" in or about September 2011. B.S. had access to a corporate bank account held at J.P. Morgan, a federally-insured financial institution.

c. K.R., an individual who resided in Texas and accepted MUSIENKO's fake employment with "Hilpert AG" in or about December 2011. K.R. had access to a bank account held at Wells Fargo & Company ("Wells Fargo"), a federally-insured financial institution.

MONEY MULE MARKETING

28. MUSIENKO engaged in money mule marketing by advertising his services to cybercriminals in Eastern Europe and elsewhere.

29. For example, from in or before January 2011 through at least on or about January 31, 2012, MUSIENKO, using the online nickname "Ply," posted online advertisements on, and sent private electronic messages through, one or more underground Russian-language cybercrime websites or "forums," where cybercriminals shared information about, and collaborated with each other in committing, various types of cybercrime. These cybercrime forums included frequent posts by individuals who had successfully hacked into U.S. bank accounts and were seeking to partner with others who could transfer the stolen funds from the hacked bank accounts in the U.S. to overseas bank accounts under their control. Conversely, the cybercrime forums also included frequent posts by individuals, like MUSIENKO, who had successfully created a network of money mules (frequently referred to as "drops") and were seeking to partner with hackers who needed help transferring stolen funds out of the hacked U.S. bank accounts. In a slight variation, these posts sometimes involved posts seeking or offering to partner with "reshippers" of stolen merchandise rather than "drops" or "money mules" of stolen funds.

30. In one post, for example, MUSIENKO, using the nickname "Ply," posted an advertisement in the Russian language on or about January 23, 2011. Translated into English, MUSIENKO stated that he had "drops in the USA," that he had corporate and personal bank accounts that were used by "drops" for online money transfers, and that he was interested in a partnership, rather than a salary job. He directed interested persons to contact him through ICQ and Jabber (popular real-time chat communications methods) at one or more specified ICQ numbers and Jabber IDs.

31. On or about January 23, 2011, MUSIENKO, using the nickname "Ply," sent private messages to other users, in which MUSIENKO advertised "drops in the USA," stating that he had 10 years' of experience, that he would keep 25% of each transaction amount for himself and that he would send 5% to his drop. MUSIENKO stated that his drops either did wire transfers or sent money online with Western Union. He stated that he was interested in a long-term partnership and again directed interested partners to contact him at a specified ICQ number or Jabber IDs.

32. From on or about March 31, 2011, through on or about January 31, 2012, MUSIENKO sent numerous similar private messages, advertising "USA drops" and personal and corporate bank accounts, claiming to have worked with drops for 10 years, and discussing his percentage share in any transactions.

THE BANK ACCOUNT TAKEOVER SCHEME

33. In or before September 2011, unidentified cybercriminal partners involved in the schemes hacked and accessed, without authorization, one or more computers belonging to Victim VDC, headquartered in Hickory, Catawba County, within the Western District of North Carolina. These members of the scheme had installed one or more malicious software programs ("malware") onto one or more of Victim VDC's computers, also located in Hickory, North Carolina. That malware recorded Victim VDC's data, including its bank account log-in credentials for its bank account at Bank #1.

34. In or about September 2011, MUSIENKO provided the cybercriminals with the bank account information for money mules J.H. and B.S. so that the bank account takeover scheme could be completed.

35. On or about September 27, 2011, unidentified cybercriminal partners involved in the schemes accessed, without authorization, a computer of Victim VDC in Hickory, North Carolina. Pretending to be Victim VDC, the cybercriminals caused that computer to access one or more computers belonging to Bank #1. Using Victim VDC's stolen account log-in credentials and other methods, these cybercriminal members of the scheme then accessed under false and fraudulent pretenses one or more bank accounts controlled by Victim VDC.

36. On or about September 27, 2011, members of the scheme in turn made an unauthorized electronic transfer of $197,526 from Victim VDC's account with Bank #1 to money mule J.H.'s corporate account with J.P. Morgan. The unauthorized electronic transfer of Victim VDC's funds under the control of Bank #1 was initiated by members of the schemes on and through one or more of Victim VDC's computers in Hickory, North Carolina.

37. On or about September 27, 2011, members of the scheme in turn made an unauthorized electronic transfer of $98,752 from Victim VDC's account with Bank #1 to money mule B.S.'s corporate account with J.P. Morgan. The unauthorized electronic transfer of Victim VDC's funds under the control of Bank #1 was initiated by members of the schemes on and through one or more of Victim VDC's computers in Hickory, North Carolina.

THE INTERNATIONAL MONEY LAUNDERING

38. On or about September 27, 2011, MUSIENKO sent an e-mail to money mule J.H. informing her that she had received a deposit into her account for $197,526.36 and that her fee of 5% amounted to $9,880, plus a $100 fee for the cost of two wire transfers. MUSIENKO directed money mule J.H. to transfer the funds she received (minus her fees) in two separate amounts to two different accounts, $108,500 to an account at HSBC Bank in London and $79,046 to an account at Barclays Bank in London.

39. On or about September 27, 2011, before money mule J.H. attempted to transfer the funds as MUSIENKO had directed, the bank detected the fraudulent transfer, notified J.H. that she had received a fraudulent transfer into her account, and returned the stolen funds to Victim VDC's bank account.

40. On or about September 27, 2011, MUSIENKO sent an e-mail to money mule B.S. informing him that he had received a deposit into his bank account of $98,752.43 and that his fee of 5% amounted to $4,940, plus a $50 fee for the cost of the wire transfer. MUSIENKO directed money mule B.S. to transfer the funds he received (minus his fees) to a specified account at HSBC Bank in London.

41. On or about September 27, 2011, acting at the direction of MUSIENKO, money mule B.S. transferred $93,767 to the designated HSBC Bank account in London.

42. On or about December 29, 2011, MUSIENKO informed money mule K.R. by phone or by e-mail that K.R. had received a deposit into his bank account of approximately $10,000. MUSIENKO directed money mule K.R. to withdraw the funds (minus his fees), take the cash to a nearby Western Union location and send the funds by wire transfer in specified dollar amounts to two individuals in various cities and countries in Eastern Europe.

43. On or about December 29, 2011, acting at the direction of MUSIENKO, money mule K.R. transferred via Western Union $4,450 to S.B. and $4,630 to O.Z., both of Kiev, Ukraine. The bank then detected the fraudulent transfer, closed the account, and seized the remaining funds in K.R.'s account.

COUNT ONE
(WIRE FRAUD - 18 U.S.C. §1343)

44. Paragraphs 1 through 43 of this Indictment are re-alleged and incorporated herein by reference as though fully set forth herein.

45. From at least in or about October 2009 through in or about March 2012, in Catawba County and Mecklenburg County, within the Western District of North Carolina, and elsewhere, the defendant,

ALEKSANDR MUSIENKO,
a/k/a "Oleksandr Serhiyovych Musiyenko,"
a/k/a "Robert Davis," a/k/a "Ply,"

and others known and unknown to the Grand Jury, with the intent to defraud, did knowingly and intentionally devise and intend to devise the above-described scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce any writing, signal or sound that affected one or more financial institutions, to wit, wire communications and unauthorized wire transfers of funds out of compromised bank accounts of Victim VDC and Other Victims to U.S.-based money-mule bank accounts, and did aid and abet other persons known and unknown to the Grand Jury.

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT TWO
(BANK FRAUD - 18 U.S.C. §1344(2))

46. Paragraphs 1 through 43 of this Indictment are re-alleged and incorporated herein by reference as though fully set forth herein.

47. From at least in or about October 2009 through in or about March 2012, in Catawba County and Mecklenburg County, within the Western District of North Carolina, and elsewhere, the defendant,

ALEKSANDR MUSIENKO,
a/k/a "Oleksandr Serhiyovych Musiyenko,"
a/k/a "Robert Davis," a/k/a "Ply,"

and others known and unknown to the Grand Jury, with the intent to defraud, did knowingly and intentionally execute and attempt to execute a scheme or artifice to obtain money under the custody and control of a financial institution, that is, Bank #1, by means of false and fraudulent pretenses, representations and promises, to wit, used stolen banking log-in credentials and Victim VDC's computers, falsely and fraudulently pretending to be Victim VDC in order to cause Bank #1 to make unauthorized wire transfers from the bank account of Victim VDC to bank accounts of money mules recruited and managed by MUSIENKO, and did aid and abet other persons known and unknown to the Grand Jury.

All in violation of Title 18, United States Code, Sections 1344(2) and 2.

COUNT THREE
(MONEY LAUNDERING CONSPIRACY – 18 U.S.C. § 1956(h))

48. Paragraphs 1 through 43 of this Indictment are re-alleged and incorporated herein by reference as though fully set forth herein.

49. From at least in or about October 2009 through in or about March 2012, in Catawba County and Mecklenburg County, within the Western District of North Carolina, and elsewhere, the defendant,

ALEKSANDR MUSIENKO,
a/k/a "Oleksandr Serhiyovych Musiyenko,"
a/k/a "Robert Davis," a/k/a "Ply,"

knowingly and intentionally conspired and agreed with other persons known and unknown to the Grand Jury to commit one or more offenses against the United States in violation of Title 18, United States Code, Sections 1956 and 1957.

Objects of the Conspiracy

50. The objects of the conspiracy for defendant **ALEKSANDR MUSIENKO** and others known and unknown to the Grand Jury were:

a. to knowingly engage and attempt to engage in one or more monetary transactions by, through and to one or more financial institutions, affecting interstate and foreign commerce, in criminally-derived property of a value greater than $10,000, that is, the withdrawal, deposit, and transfer of U.S. currency, funds, and monetary instruments out of MUSIENKO'S money mules' accounts, such property having been derived from specified unlawful activity, that is, (i) computer fraud and abuse in violation of 18 U.S.C. § 1030; (ii) wire fraud in violation of 18 U.S.C. § 1343, and (iii) bank fraud in violation of 18 U.S.C. § 1344, all in violation of 18 U.S.C. § 1957(a).

b. to transport, transmit, and transfer, and attempt to transport, transmit, and transfer one or more monetary instruments and funds involving the proceeds of specified unlawful activity, that is, (i) computer fraud and abuse in violation of 18 U.S.C. § 1030; (ii) wire fraud in violation of 18 U.S.C. § 1343, and (iii) bank fraud in violation of 18 U.S.C. § 1344, from a place in the United States to or through a place outside the United States, that is, out of MUSIENKO'S money mules' accounts to overseas recipients, knowing that the monetary instruments and funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission, and transfer was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of such specified unlawful activity, in violation of 18 U.S.C. § 1956(a)(2)(B)(i).

All in violation of Title 18, United States Code, Section 1956(h) .

COUNTS FOUR AND FIVE
(MONEY LAUNDERING - 18 U.S.C. §§ 1956(a)(2)(B)(i) and 2)

52. Paragraphs 1 through 43 of this Indictment are re-alleged and incorporated herein by reference as though fully set forth herein.

53. On or about each of the dates below, in Mecklenburg County, within the Western District of North Carolina, and elsewhere, the defendant,

ALEKSANDR MUSIENKO,
a/k/a "Oleksandr Serhiyovych Musiyenko,"
a/k/a "Robert Davis," a/k/a "Ply,"

and others known and unknown to the Grand Jury, did transport, transmit, and transfer, and attempted to transport, transmit, and transfer, monetary instruments and funds involving the proceeds of specified unlawful activity, that is, fraud in relation to computers in violation of 18 U.S.C. § 1030, wire fraud in violation of 18 U.S.C. § 1343, and bank fraud in violation of 18 U.S.C. § 1344, from a place in the United States, through Western Union servers located in the Western District of North Carolina, to or through a place outside the United States, knowing that the monetary instruments and funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission, and transfer was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of such specified unlawful activity, each instance identified below being a separate violation of 18 U.S.C. §§ 1956(a)(2)(B)(i) and 2:

COUNT	APPROXIMATE DATE	MONETARY TRANSACTION
FOUR	December 29, 2011	International money transfer of $4,450 sent via Western Union by Money Mule K.R. to S.B. located in Kiev, Ukraine.
FIVE	December 29, 2011	International money transfer of $4,630 sent via Western Union by Money Mule K.R. to O.Z. located in Kiev, Ukraine.

NOTICE OF FORFEITURE AND FINDING OF PROBABLE CAUSE

Notice is hereby given of 18 U.S.C. §§ 981, 982, 1029, and 2323, 28 U.S.C. § 2461(c), and 21 U.S.C. § 853. Under Section 2461(c), criminal forfeiture is applicable to any offenses for which forfeiture is authorized by any other statute, including but not limited to 18 U.S.C. § 981 and all specified unlawful activities listed or referenced in 18 U.S.C. § 1956(c)(7), which are incorporated as to proceeds by Section 981(a)(1)(C). The following property is subject to forfeiture in accordance with Section 981, 982, 1029, 2323, 2461(c), and/or 853:

a. All property which constitutes or is derived from proceeds obtained directly or indirectly as a result of the violations set forth in this bill of indictment;

b. All property used, or intended to be used, in any manner or part to commit or facilitate the commission of the violations; and

c. If, as set forth in 21 U.S.C. § 853(p), any property described in (a), (b), or (c) cannot be located upon the exercise of due diligence, has been transferred or sold to, or deposited with, a third party, has been placed beyond the jurisdiction of the court, has been substantially diminished in value, or has been commingled with other property which cannot be divided without difficulty, all other property of the defendant/s to the extent of the value of the property described in (a), (b), and (c).

A TRUE BILL:

[redacted]

FOREPERSON

JILL WESTMORELAND ROSE
UNITED STATES ATTORNEY

THOMAS A. O'MALLEY
ASSISTANT U.S. ATTORNEY

MONA SEDKY
SENIOR TRIAL ATTORNEY
U.S. Department of Justice, Criminal Division
Computer Crime & Intellectual Property Section