

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA : Hon.
 :
 v. : Criminal No. 09-
 :
 MAHMOUD NUSIER, : 18 U.S.C. §§ 1029, 1030, 371
 PAUL MICHAEL KWAN, and :
 NANCY GOMEZ : INDICTMENT
 :
 :

The Grand Jury in and for the District of New Jersey,
sitting in Newark, charges:

COUNT 1 - CONSPIRACY
(18 U.S.C. § 371)
(Nusier, Kwan, and Gomez)

BACKGROUND

1. At various times relevant to this Indictment:
 - a. Defendants Mahmoud Nusier, Paul Michael Kwan and Nancy Gomez resided in or about the city of Manila, Philippines and possessed telecommunications equipment.
 - b. M.Z. and S.K. were married to one another and resided in or about Brescia, Italy. They operated call centers in or about Brescia and Mascerata, Italy.
 - c. J.I. resided in or about Brescia, Italy and assisted in financing call center operations.
 - d. Y.M. resided in or about Brescia, Italy and owned and operated Madina Trading Company, located in or about Brescia, Italy.

e. AT&T was a telephone company with headquarters in Dallas, Texas, with major operating centers and a fraud detection center located in Somerset County, New Jersey.

f. Sprint was a telephone company with headquarters in Overland Park, Kansas.

g. AT&T and Sprint provided residential and business telephone service. Billing for the service was based on rate structures agreed upon by AT&T, Sprint and their customers. Calls made by AT&T's customers but not included in a particular customer's rate structure were billed at rates called the "casual dialing/premium rate." A casual dialing/premium rate was the highest rate on AT&T or Sprint's rate structure.

h. A "Call Center" was a storefront which was open to the public and contained one or more telephones for the Call Center's customers to use, akin to an Internet kiosk. Customers of the Call Center provided the terminating phone number they sought to call to the Call Center operator. The customer was then directed to a particular phone in the Call Center and the Call Center operator connected that phone to the terminating phone number. The customers of the Call Center were then billed by the minute for the phone call. Call Centers were common in Italy and Spain.

i. Large businesses and organizations commonly used private computer systems to operate their internal telephone

networks. Such an internal telephone network was referred to as a Private Branch eXchange, or "PBX." The primary functions of a PBX included making connections for internal calls placed within the system (i.e., when one employee called another employee) and connecting internal users of the system to public telephone networks, very often for the purpose of making long distance telephone calls which were then charged to the business. PBX systems directed calls made to a business' main number to the desired extension. Popular PBX systems were offered by Nortel (Meridian), Lucent, Bizfone and Panasonic.

j. Ria Financial Systems, Western Union and MoneyGram were fee-based financial services companies based in the United States which facilitated money transfers between and among individuals and businesses. These businesses did not require customers using their services to have an account, although they generally asked customers to provide personal identification information when transmitting and receiving money.

k. A "brute force attack" was a method of breaking computer codes by systematically attempting a large number of possibilities in the hope that eventually the proper code would be used. In the telecommunications context, a brute force attack consisted of systematically cycling through telephone extensions and corresponding passcodes in numeric sequence.

THE CONSPIRACY

2. From in or about October 2005 through in or about December 2008, in Manila, Philippines and Somerset County in the District of New Jersey and elsewhere, defendants

MAHMOUD NUSIER,
PAUL MICHAEL KWAN, and
NANCY GOMEZ

did knowingly and intentionally conspire and agree with each other, M.Z., S.K., J.I., Y.M., and others to commit an offense against the United States, that is:

(1) 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, and to transmit and cause the transmission by means of wire communications writings, signs, signals, and sounds in interstate and foreign commerce, namely, telephone calls and wire transfers, in furtherance of such scheme and artifice, contrary to Title 18, United States Code, Section 1343; and

(2) to access a protected computer, without authorization, and exceed authorized access, and by means of such conduct to further the intended fraud and obtain things of value, contrary to Title 18, United States Code, Section 1030(a)(4).

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy to sell telephone service to customers of Call Centers and then route the corresponding telephone calls from the Call Centers over the telephone lines of businesses and entities whose PBX systems had been hacked without having paid those businesses and entities for the routing the calls while receiving money for the calls from the customers of the Call Centers.

MANNER AND MEANS OF THE CONSPIRACY

4. It was part of the conspiracy that M.Z., S.K., J.I. and others (the "Brescia Call Center Operators") would establish call centers in Italy and Spain.

5. It was further part of the conspiracy that the Brescia Call Center Operators would hire defendants NUSIER, KWAN, GOMEZ and others in the Philippines (the "PBX Hackers") to hack PBX systems of various companies in the United States.

6. It was further part of the conspiracy that the PBX Hackers would learn the tones and operating messages of the different U.S.-based PBX systems such that they could reprogram the PBX systems remotely.

7. It was further part of the conspiracy that the PBX Hackers would search for listings and directories of business and government telephone numbers in the U.S. and elsewhere, including by acquiring telephone books. Once an entity operating a PBX

system was identified, the PBX Hackers would commence a "brute force attack" in search of either (1) unused telephone extensions of the telephone systems, or (2) telephone extensions bearing default passwords. Having identified an unused or insufficiently-protected extension, the PBX Hackers would then reprogram the extensions with new passwords (or passcodes) (the "Hacked PBX").

8. It was further part of the conspiracy that when a Hacked PBX was compromised, the PBX Hackers would assume control over the Hacked PBX. Calls could then be placed in and out of the Hacked PBX.

9. It was further part of the conspiracy that the PBX Hackers would manipulate the Hacked PBX in numerous ways, including by, (1) using a "loop-back" method, and (2) using a "passcode" method. In the "loop-back" method, the PBX Hackers and their clients would place a telephone call into a Hacked PBX and use the Hacked PBX to dial back to a second number controlled by the PBX Hackers, thereby commencing a call charged to the Hacked PBX. With the call being charged to the Hacked PBX, the Hacked PBX would then be manipulated to place calls to third parties, while maintaining an open telephone line over the PBX, causing the company that owned the Hacked PBX to incur the full costs of the call. In the "passcode" method, the PBX Hackers and their clients would place a call into the Hacked PBX and then,

using a passcode learned from the brute force attack, manipulate the Hacked PBX to dial calls to third parties located in dialing areas with significantly more expensive dialing rates than the initial calls to the Hacked PBX (e.g., Cuba). In this "passcode" method, the PBX Hackers would still be charged by their own long distance carrier for the initial call into the Hacked PBX, but the rate for such a call would be less than the rate to the ultimate destination, which was charged to the owner of the Hacked PBX.

10. It was further part of the conspiracy that the PBX Hackers would transmit the Hacked PBX number, extensions and passcodes to the Brescia Call Center Operators.

11. It was further part of the conspiracy that the Brescia Call Center Operators would transmit money to the PBX Hackers by electronic wire transfers facilitated by Y.J.'s business, Madina Trading Company, often using Western Union, Ria Financial Systems, and MoneyGram, as payment for hacking into the PBX systems.

12. It was further part of the conspiracy that the Brescia Call Center Operators would transmit the Hacked PBX number, extensions and passcodes to operators of Call Centers elsewhere, including Spain, in return for payment.

The Call Centers

13. It was further part of the conspiracy that the Brescia Call Center Operators and others located in Italy would use the Hacked PBX information provided by defendants NUSIER, KWAN and GOMEZ to route calls from the Call Centers to the termination numbers where their Call Center customers wished to be connected. Through this method of operation, more than approximately twelve million minutes of telephone calls, totaling more than approximately \$55,000,000 in telephone charges, were made through the Hacked PBX systems of entities including businesses in New Jersey.

OVERT ACTS

14. In furtherance of the conspiracy and to effect its unlawful object, the defendants MAHMOUD NUSIER, PAUL MICHAEL KWAN, NANCY GOMEZ, M.Z., S.K., J.I., Y.M. and others committed and caused to be committed the following overt acts in the District of New Jersey and elsewhere:

Payments in Furtherance of the Conspiracy

- a. On or about October 4, 2005, through Madina Trading Company, J.I. sent an approximately \$900 Western Union money transfer to defendant MAHMOUD NUSIER.
- b. On or about October 24, 2005, through Madina Trading Company, J.I. sent an approximately \$120 Western Union money transfer to defendant PAUL MICHAEL KWAN.
- c. On or about November 29, 2005, through Madina Trading Company, M.Z. sent an approximately \$100 Western Union money transfer to defendant MAHMOUD NUSIER.
- d. On or about February 26, 2007, through Madina Trading Company, M.Z. sent an approximately \$100 Western Union money transfer to defendant PAUL MICHAEL KWAN.
- e. On or about February 28, 2007, through Madina Trading Company, M.Z. sent an approximately \$50 Western Union money transfer to defendant MAHMOUD NUSIER.

Calls in Furtherance of the Conspiracy

f. On or about January 23, 2006, at approximately 11:26:55 EST, M.Z. caused an outbound call to be made from the telephone number 609-XXX-3189, belonging to a Hightstown, New Jersey company identified herein as "C.D.," to M.Z.'s Call Center in Brescia, Italy (the "11:26 Call"). The call remained connected for over seventeen minutes without C.D.'s authorization.

g. On or about December 22, 2007, at approximately 16:45:16 EST, a call was placed from M.Z.'s Call Center in Brescia, Italy to the telephone number 212-XXX-3452 carried by AT&T (the "16:45 Call"), an extension belonging to a Purchase, New York company identified herein as A.M. (the "A.M. PBX"). At approximately 16:47:16, while the 16:45 Call was ongoing, a call was made using the "passcode" method from the A.M. PBX to a number in Cuba.

h. On or about December 23, 2007, at approximately 3:55:31 A.M. EST, a call was made from M.Z.'s Call Center in Brescia, Italy to the A.M. PBX (the "3:55 Call"). While the 3:55 Call was ongoing, a call was made using the "loop-back" method from the A.M. PBX back to M.Z.'s call center.

i. On or about February 13, 2008, at approximately 13:33:46 EST, a call was made from M.Z.'s Call Center to the telephone number 281-XXX-7100, carried by AT&T (the "13:33 Call"), an extension belonging to a Greens Crossing, Texas

company identified herein as H.L. (the "H.L. PBX"). At approximately 13:57:31, while the 13:33 Call was ongoing, a call was made using the "passcode" method from the H.L. PBX to a number in Cuba.

j. On or about February 13, 2008 at approximately 13:56:49 EST, a call was made from M.Z.'s Call Center back to the H.L. PBX (the "13:56 Call"). At approximately 13:57:31, while the 13:56 Call was ongoing, a call was made using the "passcode" method from the H.L. PBX to a number in Senegal.

k. On or about March 10, 2007, defendants NUSIER, KWAN and GOMEZ possessed, without authorization, documents containing telephone numbers, extensions and passcodes to PBX systems of businesses in the District of New Jersey and elsewhere.

In violation of Title 18, United States Code, Section 371.

Count 2: UNAUTHORIZED ACCESS TO A PROTECTED COMPUTER
(18 U.S.C. § 1030)
(Mahmoud Nusier)

1. The allegations set forth in paragraph 1 and paragraphs 3 through 14 of Count One of this Indictment are realleged and incorporated herein.

2. On or about August 13, 2005, at approximately 5:51 A.M. EST, defendant NUSIER made an unauthorized call from the PBX of a company identified herein as "G.M.," of Seattle, Washington (the "G.M. PBX"), to his home telephone number in the Philippines. The unauthorized call remained connected for approximately 1,394 minutes (23 hours and 14 minutes), during which time defendant NUSIER remained in control of the G.M. PBX. During this period, multiple unauthorized calls were made using the "loop-back" method from the G.M. PBX to numbers in Guinea.

3. On or about August 13, 2005, G.M.'s long distance telephone calls were serviced by AT&T.

4. On or about August 13, 2005, in Somerset County in the District of New Jersey, and elsewhere, defendant

MAHMOUD NUSIER

did knowingly and with intent to defraud, access a protected computer, namely, the G.M. PBX, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained something of value.

In violation of Title 18, United States Code, Section 1030(a)(4) and Section 2.

Count 3: UNAUTHORIZED ACCESS TO A PROTECTED COMPUTER
(18 U.S.C. § 1030)
(Mahmoud Nusier)

1. The allegations set forth in paragraph 1 and paragraphs 3 through 14 of Count One are realleged and incorporated herein.

2. On or about February 10, 2007, at approximately 23:12 P.M. EST, defendant NUSIER made an unauthorized call from the PBX of a company identified herein as "A.K.," of Alpharetta, Georgia (the "A.K. PBX"), to his home telephone number in the Philippines. The call remained connected for approximately 2,087 minutes (34 hours and 47 minutes), during which time defendant NUSIER remained in control of the A.K. PBX. During this period, multiple unauthorized calls were made using the "loop-back" method from the A.K. PBX to numbers in the United States.

3. On or about February 10, 2007, A.K.'s long distance telephone calls were serviced by AT&T.

4. On or about February 10, 2007, in Somerset County in the District of New Jersey, and elsewhere, defendant

MAHMOUD NUSIER

did knowingly and with intent to defraud, access a protected computer, namely, the A.K. PBX, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained something of value.

In violation of Title 18, United States Code, Section 1030(a)(4) and Section 2.

Count 4: UNAUTHORIZED ACCESS TO A PROTECTED COMPUTER
(18 U.S.C. § 1030)
(Paul Michael Kwan)

1. The allegations set forth in paragraph 1 and paragraphs 3 through 14 of Count One of this Indictment are realleged and incorporated herein.

2. On or about January 22, 2007, at approximately 5:10 A.M. EST, defendant KWAN made an unauthorized call from the PBX of a company identified herein as "M.S.," of Upland, California (the "M.S. PBX"), to his home telephone number in the Philippines. The call remained connected for approximately 478 minutes (7 hours and 58 minutes), during which time defendant KWAN remained in control of the M.S. PBX. During this period, multiple unauthorized calls were made using the "loop-back" method from the M.S. PBX to other numbers in the Philippines.

3. On or about January 22, 2007, M.S.'s long distance telephone calls were serviced by AT&T.

4. On or about January 22, 2007, in Somerset County in the District of New Jersey, and elsewhere, defendant

PAUL MICHAEL KWAN,

did knowingly and with intent to defraud, access a protected computer, namely, the M.S. PBX, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained something of value.

In violation of Title 18, United States Code, Section 1030(a)(4) and Section 2.

Count 5: UNAUTHORIZED ACCESS TO A PROTECTED COMPUTER
(18 U.S.C. § 1030)
(Paul Michael Kwan)

1. The allegations set forth in paragraph 1 and paragraphs 3 through 14 of Count One of this Indictment are realleged and incorporated herein.

2. On or about November 19, 2005, at 8:14 A.M. EST, defendant KWAN made an unauthorized call from the PBX of a company identified herein as "A.I.," of San Jose, California (the "A.I. PBX"), to his home telephone number in the Philippines. The call remained connected for approximately 1,327 minutes (22 hours and 8 minutes), during which time defendant KWAN remained in control of the A.I. PBX. During this period, multiple unauthorized calls were made using the "loop-back" method from the A.I. PBX to other numbers in the Philippines.

3. On or about November 19, 2005, A.I.'s long distance telephone calls were serviced by AT&T.

4. On or about November 19, 2005, in Somerset County in the District of New Jersey, and elsewhere, defendant

PAUL MICHAEL KWAN,

did knowingly and with intent to defraud, access a protected computer, namely, the A.I. PBX, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained something of value.

In violation of Title 18, United States Code, Section 1030(a)(4) and Section 2.

Count 6: UNAUTHORIZED ACCESS TO A PROTECTED COMPUTER
(18 U.S.C. § 1030)
(Nancy Gomez)

1. The allegations set forth in paragraph 1 and paragraphs 3 through 14 of Count One of this Indictment are realleged and incorporated herein.

2. On or about June 24, 2006, at approximately 1:21 A.M. EST, defendant GOMEZ made an unauthorized call from the PBX of a company identified herein as "A.S.," of Valley Stream, New York (the "A.S. PBX"), to her home telephone number in the Philippines. The call remained connected for approximately 271 minutes (4 hours and 31 minutes), during which time defendant GOMEZ remained in control of the A.S. PBX. During this period, multiple unauthorized calls were made using the "loop-back" method from the A.S. PBX to numbers in India.

3. On or about June 24, 2006, A.S.'s long distance telephone calls were serviced by AT&T.

4. On or about June 24, 2006, in Somerset County in the District of New Jersey, and elsewhere, defendant

NANCY GOMEZ

did knowingly and with intent to defraud, access a protected computer, namely the A.S. PBX, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained something of value.

In violation of Title 18, United States Code, Section 1030(a)(4) and Section 2.

Count 7: UNAUTHORIZED ACCESS TO A PROTECTED COMPUTER
(18 U.S.C. § 1030)
(Nancy Gomez)

1. The allegations set forth in paragraph 1 and paragraphs 3 through 14 of Count One of this Indictment are realleged and incorporated herein.

2. On or about August 21, 2006, at 9:55 A.M. EST, defendant GOMEZ made an unauthorized call from the PBX of a company identified herein as "A.S.A.," of Washington, D.C. (the "A.S.A. PBX"), to her home telephone number in the Philippines. The call remained connected for approximately 1,378 minutes (22 hours and 58 minutes), during which time defendant GOMEZ remained in control of the A.S.A. PBX. During this period, an unauthorized call was made using the "loop-back" method from the A.S.A. PBX to a number in the United States.

3. On or about August 21, 2006, A.S.A.'s long distance telephone calls were serviced by AT&T.

4. On or about August 21, 2006, in Somerset County in the District of New Jersey, and elsewhere, defendant

NANCY GOMEZ

did knowingly and with intent to defraud, access a protected computer, namely, the A.S.A. PBX, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained something of value.

In violation of Title 18, United States Code, Section 1030(a)(4) and Section 2.

Count 8: ACCESS DEVICE FRAUD - MULTIPLE ACCESS DEVICES
(18 U.S.C. § 1029(a)(3))
(Nusier, Kwan, and Gomez)

1. The allegations set forth in paragraph 1 and paragraphs 3 through 14 of Count One of this Indictment are realleged and incorporated herein.

2. On or about March 10, 2007, defendants NUSIER, KWAN and GOMEZ possessed, without authorization, documents containing telephone numbers, extensions and passcodes to PBX systems of businesses in the District of New Jersey and elsewhere.

3. On or about March 10, 2007, in the Philippines, the District of New Jersey, and elsewhere, defendants

MAHMOUD NUSIER,
PAUL MICHAEL KWAN,
NANCY GOMEZ

did knowingly and with intent to defraud possess fifteen or more unauthorized access devices, namely passcodes corresponding to telephone numbers and extensions, in a manner affecting foreign commerce, by facilitating unauthorized international and other telephone calls through U.S.-based telephone systems.

In violation of Title 18, United States Code, Section
1029(a)(3) and Section 2.

A TRUE BILL

FOREPERSON

Ralph J. Marra, Jr.
RALPH J. MARRA, JR.
ACTING UNITED STATES ATTORNEY

CASE NUMBER: _____

**United States District Court
District of New Jersey**

UNITED STATES OF AMERICA

v.

**MAHMOUD NUSIER,
PAUL MICHAEL KWAN, and
NANCY GOMEZ**

INDICTMENT FOR

18 U.S.C. §§ 371, 1030, 1029, and 2

A True Bill,

Foreperson

RALPH J. MARRA, JR.
ACTING U.S. ATTORNEY NEWARK, NEW JERSEY

EREZ LIEBERMANN
ASSISTANT U.S. ATTORNEY
(973) 645-2874

USAO#2005R00946