UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - - - -X

UNITED STATES OF AMERICA	:	**SEALED INDICTMENT**
-v.-	:	S4 12 Cr. 487
DENISS ČALOVSKIS, a/k/a "Miami,"	:	
Defendant.	:	

- - - - - - - - - - - - - - - - - - - -x

COUNT ONE

(Bank Fraud Conspiracy)

The Grand Jury charges:

INTRODUCTION

1. From at least in or about 2005, up to and including in or about March 2012, in the Southern District of New York and elsewhere, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, conspired to steal personal information that was used to access bank and other accounts online from over a million victims, including from individuals, government entities and businesses in the United States and elsewhere using malicious computer code, or malware, known as the "Gozi Virus." The stolen information was then used to steal millions of dollars from those bank accounts.

2. The Gozi Virus was named by private sector information security experts in the United States who, in or about 2007, discovered that a previously unrecognized malicious

computer code was stealing personal bank account information (such as account numbers, usernames, and passwords) from computers across Europe on a vast scale, while remaining virtually undetectable in the computers it infected. Beginning at least in or about 2010, the Gozi Virus spread to the United States.

3. The Gozi Virus was distributed and delivered to victims' computers in different ways. In one method, for example, the virus was disguised as an apparently benign .pdf document (i.e., a document in the widely used .pdf format, which is easily shared among different computer operating systems). When a victim opened the .pdf document, the Gozi Virus was secretly installed onto the victim's computer, where it was generally undetectable by anti-virus software. Once installed, the Gozi Virus collected data from the infected computer in order to capture the victim's bank account user name, password, and other vital security information, and sent that data to a computer server controlled by certain users of the Gozi Virus who used the data fraudulently to transfer funds out of the victim's account and, ultimately, into their personal possession. Since its inception, the Gozi Virus has infected well over a million computers around the world, including at least 17,000 computers in the United States, of which more than 160 were computers belonging to the National Aeronautics and Space Administration

("NASA"). The Gozi Virus has caused, at a minimum, millions of dollars in losses.

THE DEFENDANT AND THE SCHEME TO DEFRAUD

4. At all times relevant to this Indictment, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, was a citizen and resident of Latvia. ČALOVSKIS had training and expertise in computer programming.

5. Beginning in or about 2005, a co-conspirator not named as a defendant herein ("CC-1") began to design the Gozi Virus to steal the online banking credentials of individuals and businesses on a widespread basis, which information CC-1 could then use to obtain money from those bank accounts. CC-1 created a list of technical specifications for the Gozi Virus, and relied on another co-conspirator not named as a defendant herein ("CC-3") to write the Virus's "source code," the set of computer instructions enabling the Virus to operate.

6. Thereafter, as part of the fraudulent scheme, in or about 2006, CC-1 began, among other things, to provide the Gozi Virus to co-conspirators on a rental basis for a fee through an operation he termed "76 Service." In particular, through "76 Service," CC-1 enabled co-conspirators, on their own, to configure the Gozi Virus to steal varying types of data (for example, passwords, usernames, or other security credentials), and to launch the Gozi Virus to attack victims' computers,

causing those computers to send the stolen data to a particular computer server controlled by CC-1. For a fee, CC-1 gave each co-conspirator access for a period of time to the specific data stolen as a result of that co-conspirator's "rental" of the virus. CC-1 advertised "76 Service" on one or more Internet forums devoted to cybercrime and other criminal activities. Another co-conspirator not named as a defendant herein ("CC-2") was one of the individuals who rented the Gozi Virus from CC-1 beginning in or about 2008.

7. In or about 2008, following various operational and technical difficulties, CC-1 ceased renting the Gozi Virus through "76 Service." Thereafter, in or about 2009, CC-1 began to sell the Gozi Virus to various co-conspirators. Among these co-conspirators was a group of individuals who sought to use the Gozi Virus to attack computers and steal money from bank accounts in the United States on a widespread basis, as well as individuals who sought to use the Gozi Virus for similar purposes in certain European countries.

8. As a further part of the fraudulent scheme, beginning in or about 2009, CC-2 became CC-1's partner in the distribution of the Gozi Virus. CC-2 worked with CC-1, among other ways, to sell or rent the Gozi Virus to other co-conspirators. CC-1 and CC-2 shared the proceeds derived from such distribution of the Gozi Virus.

9. As a further part of the fraudulent scheme, CC-2 hired another co-conspirator not named as a defendant herein ("CC-4") to develop an updated version of the Gozi Virus. CC-4 also provided technical support for the updated Gozi Virus, including, among other ways, regularly refining and updating the obfuscation software that was used to conceal the Gozi Virus from detection by antivirus software on victims' computers.

10. As a further part of the fraudulent scheme, CC-4 also hired DENISS ČALOVSKIS, a/k/a "Miami," the defendant, to develop computer code, known as web injects, which altered how particular banking websites appeared on infected computers in order to deceive victims into divulging additional personal information, such as mother's maiden name. The personal information was then surreptitiously transmitted to other co-conspirators and used to access and steal funds from the victims' accounts. ČALOVSKIS developed web injects not only for the Gozi Virus, but also for other banking malware, such as the Zeus Trojan.

11. Attached as Exhibit A to this Indictment is an illustration of a web inject supplied by ČALOVSKIS. The first page of Exhibit A depicts the account summary web page that an online banking customer with a bank headquartered in Manhattan, New York ("Bank-1") would have seen when accessing that web page from an uninfected computer. In contrast, the second page of

Exhibit A shows how the same web page would have been modified by ČALOVSKIS's web inject to request additional identity information not required by Bank-1 from the account holder, including, among other things, mother's maiden name, social security number, driver's license number, date of birth, and automated teller machine (ATM) card number.

STATUTORY ALLEGATIONS

12. From at least in or about 2005, up to and including in or about June 2012, in the Southern District of New York and elsewhere, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit bank fraud, in violation of Title 18, United States Code, Section 1344.

13. It was a part and an object of the conspiracy that DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, willfully and knowingly would and did execute a scheme and artifice to defraud a financial institution, the accounts and deposits of which were then insured by the Federal Deposit Insurance Corporation, and to obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, a financial institution, by means of false and fraudulent pretenses, representations, and

promises, in violation of Title 18, United States Code, Section 1344.

Overt Acts

14. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about January 8, 2009, CC-1 offered to sell access to the Gozi Virus to a co-conspirator not named as a defendant herein ("CC-6").

b. On or about June 19, 2010, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, told another co-conspirator not named as a defendant herein ("CC-7") that he (ČALOVSKIS) had "injects" for both the Gozi Virus and the Zeus Trojan.

c. By at least in or about October 2010, a computer belonging to a business located in Manhattan, New York, had been infected with the Gozi Virus.

d. On or about September 13, 2010, CC-4 told CC-2 that CC-2's payment for technical support for the Gozi Virus had run out. CC-2 responded by sending more money and asked CC-4 for new obfuscation software for the Gozi Virus.

e. On or about January 9, 2011, CC-3 sent an instant message containing a link to a file with a version of the Gozi Virus.

(Title 18, United States Code, Section 1349.)

COUNT TWO

(Access Device Fraud Conspiracy)

The Grand Jury further charges:

15. The allegations contained in paragraphs 1 through 11 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

16. From at least in or about 2005, up to and including in or about June 2012, in the Southern District of New York and elsewhere, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit access device fraud offenses, in violation of Title 18, United States Code, Sections 1029(a)(2) and (a)(3).

17. It was a part and an object of the conspiracy that DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, knowingly and with intent to defraud, as part of an offense affecting interstate and foreign commerce, would and did traffic in and use one and more unauthorized access devices during any one-year period, and by such conduct would and did obtain anything of value aggregating $1,000 and more during that

period, in violation of Title 18, United States Code, Section 1029(a)(2).

18. It was a further part and an object of the conspiracy that DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, knowingly and with intent to defraud, as part of an offense affecting interstate and foreign commerce, would and did possess fifteen and more devices which were counterfeit and unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

Overt Acts

19. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about January 8, 2009, CC-1 offered to sell access to the Gozi Virus to CC-6.

b. In or about September 2010, CC-4 told CC-2 that CC-2's payment for technical support for the Gozi Virus had run out. CC-2 responded by sending more money and asked CC-4 for new obfuscation software for the Gozi Virus.

c. By at least in or about October 2010, a computer belonging to a business located in Manhattan, New York, had been infected with the Gozi Virus.

d. In or about late 2010, members of the conspiracy controlled a command and control server for the Gozi Virus that stored over 3,000 user names of customers of approximately seven U.S. banks, among others.

e. On or about January 9, 2011, CC-3 sent an instant message containing a link to a file with a version of the Gozi Virus.

f. In or about January 2011, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, sold a web inject that was designed to be used with the Gozi Virus to fraudulently obtain personal information, such as social security numbers and ATM card numbers, from online banking customers.

g. In or about February 2012, over $200,000 was fraudulently transferred out of a bank account controlled by a victim ("Victim-1") whose computer had been infected with the Gozi Virus.

(Title 18, United States Code, Section 1029(b)(2).)

COUNT THREE

(Conspiracy to Commit Computer Intrusion)

The Grand Jury further charges:

20. The allegations contained in paragraphs 1 through 11 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

21. From at least in or about 2005, up to and including in or about June 2012, in the Southern District of New York and elsewhere, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit computer intrusion offenses in violation of Title 18, United States Code, Sections 1030(a)(2), (a)(4), (a)(5)(A) and (a)(6).

22. It was a part and an object of the conspiracy that DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, would and did intentionally access computers without authorization, and thereby would and did obtain information from protected computers, for purposes of commercial advantage and private financial gain, and in furtherance of criminal and tortious acts in violation of the Constitution and the laws of the United States, and the value of the information obtained exceeded $5,000, in violation of Title 18, United States Code, Section 1030(a)(2).

23. It was a further part and an object of the conspiracy that DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, knowingly and with intent to defraud, would and did access protected computers without authorization, and by means of such conduct would and did further

the intended fraud and obtain anything of value, in violation of Title 18, United States Code, Section 1030(a)(4).

24. It was a further part and an object of the conspiracy that DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, knowingly would and did cause the transmission of a program, information, code, and command, and as a result of such conduct, would and did intentionally cause damage without authorization, to protected computers, in violation of Title 18, United States Code, Section 1030(a)(5)(A).

25. It was a further part and an object of the conspiracy that DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, in transactions affecting interstate and foreign commerce, and computers used by and for the Government of the United States, knowingly and with intent to defraud trafficked in passwords and similar information through which computers may be accessed without authorization, in violation of Title 18, United States Code, Section 1030(a)(6).

Overt Acts

26. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. From in or about 2008 to in or about June 2012, over 160 NASA computers were infected with the Gozi Virus, resulting in over $40,000 in damage.

b. On or about January 8, 2009, CC-1 offered to sell access to the Gozi Virus to CC-6.

c. On or about June 19, 2010, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, told CC-7 that he (ČALOVSKIS) had "injects" for both the Gozi Virus and the Zeus Trojan.

d. In or about September 2010, CC-4 told CC-2 that CC-2's payment for technical support for the Gozi Virus had run out. CC-2 responded by sending more money and asked CC-4 for new obfuscation software for the Gozi Virus.

e. By at least in or about October 2010, a computer belonging to a business located in Manhattan, New York, had become infected with the Gozi Virus.

f. In or about late 2010, members of the conspiracy controlled a command and control server for the Gozi Virus that stored over 3,000 user names of customers of approximately seven U.S. banks, among others.

g. On or about January 9, 2011, CC-3 sent an instant message containing a link to a file with a version of the Gozi Virus.

(Title 18, United States Code, Sections 1030(b), (c)(2)(B) and (c)(4)(B).)

COUNT FOUR

(Wire Fraud Conspiracy)

The Grand Jury further charges:

27. The allegations contained in paragraphs 1 through 11 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

28. From at least in or about 2005, up to and including in or about June 2012, in the Southern District of New York and elsewhere, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

29. It was a part and an object of the conspiracy that DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, willfully and knowingly would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

Overt Acts

30. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about January 8, 2009, CC-1 offered to sell access to the Gozi Virus to CC-6.

b. On or about June 19, 2010, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, told CC-7 that he (ČALOVSKIS) had "injects" for both the Gozi Virus and the Zeus Trojan.

c. In or about September 2010, CC-4 told CC-2 that CC-2's payment for technical support for the Gozi Virus had run out. CC-2 responded by sending more money and asked CC-4 for new obfuscation software for the Gozi Virus.

d. By at least in or about October 2010, a computer belonging to a business located in Manhattan, New York, had been infected with the Gozi Virus.

e. On or about January 9, 2011, CC-3 sent an instant message containing a link to a file with a version of the Gozi Virus.

(Title 18, United States Code, Section 1349.)

COUNT FIVE

(Conspiracy to Commit Aggravated Identity Theft)

The Grand Jury further charges:

31. The allegations contained in paragraphs 1 through 11 above are hereby repeated, realleged, and incorporated by reference as if fully set forth herein.

32. From at least in or about 2005, up to and including in or about June 2012, in the Southern District of New York and elsewhere, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, to commit aggravated identity theft in violation of Title 18, United States Code, Section 1028A.

33. It was a part and an object of the conspiracy that DENISS ČALOVSKIS, a/k/a "Miami," the defendant, and others known and unknown, during and in relation to any felony violation enumerated in Title 18, United States Code, Section 1028A, to wit, the offenses charged in Counts One, Two and Four of this Indictment, knowingly would and did transfer, possess, and use, without lawful authority, means of identification of other persons, in violation of Title 18, United States Code, Section 1028A.

Overt Acts

34. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about January 8, 2009, CC-1 offered to provide CC-6 with access to the Gozi Virus.

b. In or about September 2010, CC-4 told CC-2 that CC-2's payment for technical support for the Gozi Virus had run out. CC-2 responded by sending more money and asked CC-4 for new obfuscation software for the Gozi Virus.

c. By at least in or about October 2010, a computer belonging to a business located in Manhattan, New York, had been infected with the Gozi Virus, and the user name of a victim ("Victim-2") who used that computer had been transmitted to a Gozi command and control server.

d. On or about January 9, 2011, CC-3 sent an instant message containing a link to a file with a version of the Gozi Virus.

e. In or about January 2011, DENISS ČALOVSKIS, a/k/a "Miami," sold a web inject that was designed to be used with the Gozi Virus to fraudulently obtain personal information,

including social security numbers, ATM numbers and driver's license numbers, from online banking customers.

(Title 18, United States Code, Section 371.)

FORFEITURE ALLEGATIONS AS TO COUNTS ONE, TWO AND FOUR

35. As a result of committing the bank fraud conspiracy offense alleged in Count One, the access device fraud conspiracy offense alleged in Count Two, and/or the wire fraud conspiracy offense alleged in Count Four of this Indictment, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461, all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the offenses, including but not limited to, at least approximately $50 million, representing the amount of proceeds obtained as a result of the offenses charged in Counts One, Two and Four.

Substitute Assets Provision

36. If any of the above-described forfeitable property, 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, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 981, 1029, 1343, 1344, and 1349; Title 28, United States Code, Section 2461; and Title 21, United States Code, Section 853.)

FORFEITURE ALLEGATION AS TO COUNT THREE

37. As a result of committing the computer intrusion conspiracy offense alleged in Count Three of this Indictment, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, shall forfeit to the United States,

(a) pursuant to 18 U.S.C. § 982(a)(2)(B), any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense, including but not limited to at least approximately $50 million, a sum of money representing the amount of proceeds obtained as a result of the offense charged in Count Three; and

(b) pursuant to 18 U.S.C. § 1029(c)(1)(C), any personal property used or intended to be used to commit the offense charged in Count Three.

Substitute Assets Provision

38. If any of the above-described forfeitable property, 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, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of the defendant up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 982 and 1030, and Title 21, United States Code, Section 853.)

FORFEITURE ALLEGATION AS TO COUNT FIVE

39. As a result of committing the aggravated identity theft conspiracy offense alleged in Count Five of this

Indictment, DENISS ČALOVSKIS, a/k/a "Miami," the defendant, shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(2)(B) and 18 U.S.C. § 1028(b)(5), all personal property used or intended to be used, in any manner or part, to commit or facilitate the commission of the offense charged in Count Five.

Substitute Assets Provision

40. If any of the above-described forfeitable property, 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, pursuant to 18 U.S.C. § 982(b), to seek forfeiture of any other property of the

defendant up to the value of the above-described forfeitable property.

(Title 18, United States Code, Sections 982, 1028(b)(5), 1028A; Title 28, United States Code, Section 2461; and Title 21, United States Code, Section 853.)

[redacted]

PREET BHARARA
United States Attorney

EXHIBIT A

#REDACTED# Online Logo

#REDACTED#.com | Contact Us | Site Feedback | Privacy Notice | LOG OFF

Payments & Transfers Products & Services Customer Center

#REDACTED# ONLINE℠ Tuesday, April 17, 2012

Print

Welcome #REDACTED#

Secure Message Center | Customize Accounts

#REDACTED# | Last logged on at 11:06 AM ET on 04/03/2012 | See session summary

Wire Money Payroll

Account Summary

Business Accounts

Deposit accounts	**$#REDACTED#**

Create a list of your favorite accounts

Business Accounts

Deposit Accounts

Total balance: $#REDACTED#

Account		
BUSINESS CLASSIC #REDACTED#	Present balance	**$#REDACTED#**
	Available balance	$#REDACTED#

See statements Make a transfer Deposit checks

#REDACTED# Debit Card Bonus Offers — Show Offers

Payments & Transfers

- Make a transfer
- Pay bills
- Add a payee
- Wire money
- Go to Payments & Transfers

Customer Center

- Try #REDACTED# Mobile
- Manage Account Alerts
- Change my Password
- Change mailing address, phone and/or email
- Stop payment on a check
- Delegate with Access Manager℠
- Go to Download Center
- Go to Customer Center

#REDACTED# strictly prohibits the use of any account to conduct any transactions that are directly or indirectly related to unlawful Internet gambling or any other illegal activity. The customer agrees not to conduct any transactions through the account that directly or indirectly involve or are related to unlawful Internet gambling, including, without limitation, the acceptance or receipt of any funds or deposits in connection therewith.

#REDACTED# Online Logo

#REDACTED#.com | Contact Us | Site Feedback | Privacy Notice | LOG OFF

Payments & Transfers Products & Services Customer Center

#REDACTED# ONLINE℠ Tuesday, April 17, 2012

Print

Welcome #REDACTED#

Secure Message Center Customize Accounts

#REDACTED# | Last logged on at 11:08 AM ET on 04/03/2012 | See session summary

In order to provide you with extra security, we occasionally need to ask for additional information when you access your accounts online.

Please enter the information below to continue.

Mother's Maiden Name:

Social Security Number: - - (xxx-xx-xxxx)

Drivers License:

Exp. Date: - - (mm-dd-yyyy)

Date of Birth: - - (mm-dd-yyyy)

ATM Card Number:

Exp.Date: / (mmyyyy)

PIN Code:

CVV Code:

Wire Money Payroll

Payments & Transfers

- Make a transfer
- Pay bills
- Add a payee
- Wire money
- Go to Payments & Transfers

Customer Center

- Try #REDACTED# Mobile
- Manage Account Alerts
- Change my Password
- Change mailing address, phone and/or email
- Stop payment on a check
- Delegate with Access Manager℠
- Go to Download Center
- Go to Customer Center

Account Summary

Business Accounts

Deposit accounts $#REDACTED#

Create a list of your favorite accounts

Business Accounts

Deposit Accounts

Total balance:#REDACTED#

Account

BUSINESS CLASSIC (#REDACTED#)

Present balance $#REDACTED#
Available balance $#REDACTED#

See statements Make a transfer Deposit checks

#REDACTED# Debit Card Bonus Offers Show Offers

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

DENISS ČALOVSKIS,
a/k/a "Miami,"

Defendant.

SEALED INDICTMENT

S4 12 Cr. 487

(18 U.S.C. §§ 371, 1029(b)(2), 1030(b) and 1349)

PREET BHARARA
United States Attorney.

A TRUE BILL

[redacted]