UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA

v. Mag. No. 23-11200 (AME)

FERAS KHALIL AHMAD ALBASHITI
a/k/a "r1z,"
a/k/a "Feras Bashiti," and
a/k/a "Firas Bashiiti"

AFFIDAVIT

I, David E. Malagold, being duly sworn, hereby depose and state:

1. I am a citizen of the United States of America and a resident of the State of New Jersey. I have been employed as an Assistant United States Attorney in the United States Attorney's Office for the District of New Jersey since May 2006. My duties include the prosecution of persons charged with violations of the criminal laws of the United States. Based upon my training and experience, I have become knowledgeable in the criminal laws and procedures of the United States.

2. In the course of my official duties, I have become familiar with the charges and evidence in the case against FERAS KHALIL AHMAD ALBASHITI, also known as "r1z," "Feras Bashiti," and "Firas Bashiti," entitled *United States v. Feras Khalil Ahmad AlBashiti,* Mag. Number 23-11200 (AME), which arose out of an investigation by the Federal Bureau of Investigation (FBI).

THE CHARGES AND RELEVANT UNITED STATES LAW

3. On December 6, 2023, United States Magistrate Judge André M. Espinosa, sitting in the United States District Court for the District of New Jersey, issued a three-count Superseding Criminal Complaint, Mag. No. 23-11200 (AME), charging AlBashiti with the crimes listed below:

Count	Crime	Statutory Citation	Maximum Penalty
One	Fraud and related activity in connection with computers	18 U.S.C. § 1030(a)(6)(A)	1 year imprisonment, $100,000 fine, 1 year supervised release, $100 special assessment
Two	Fraud and related activity in connection with access devices	18 U.S.C. § 1029(a)(5)	15 years' imprisonment, $250,000 fine, 3 years supervised release, $100 special assessment
Three	Fraud and related activity in connection with access devices	18 U.S.C. § 1029(a)(2)	10 years' imprisonment, $250,000 fine, 3 years supervised release, $100 special assessment

4. A complaint is a charging document that alleges violations of the criminal laws of the United States. Under United States law, in order for a complaint to issue, a United States Magistrate Judge must review a sworn statement of a law enforcement officer regarding the essential facts concerning the offense charged—in this case, a sworn statement of Federal Bureau of Investigation Task Force Officer Baker—and determine whether there is probable cause to believe that a crime has been committed and that the defendant committed the crime.

5. If AlBashiti's extradition to the United States is granted, another charging document, called an indictment, will be sought from a federal grand jury sitting in the District of New Jersey, unless AlBashiti waives indictment. If AlBashiti waives indictment, the United States Attorney for the District of New Jersey will issue a charging document called an information. The indictment or information, which would supersede the criminal complaint, would only include the offenses as alleged in the criminal complaint and as set forth above.

6. Based on the charges in the Superseding Complaint, on December 6, 2023, the United States District Court for the District of New Jersey issued an arrest warrant for AlBashiti. This arrest warrant remains valid and executable to bring AlBashiti before the Court to stand trial. It is the practice of the United States District Court for the District of New Jersey to retain original documents and warrants to file them with the Clerk of the Court. Therefore, I have obtained certified true and accurate copies of the December 6, 2023, Superseding Complaint and arrest warrant from the Clerk of the Court and have attached them to this affidavit as **Exhibit A** and **Exhibit B**, respectively.

7. The relevant portions of the statutes cited above are attached to this affidavit as **Exhibit C**. Each of these statutes was duly enacted and in force at the time the offenses were committed and at the time the Superseding Complaint was filed, and they remain in full force and effect. A violation of Count One constitutes a

misdemeanor under the laws of the United States. A violation of Counts Two and Three constitutes a felony under the laws of the United States.

8. Regarding Count One of the Superseding Complaint (18 U.S.C. § 1030(a)(6)(A)), the United States must prove: (1) that AlBashiti knowingly and without authorization trafficked in a password, or similar information through which a computer may be accessed; (2) that AlBashiti acted with intent to defraud; and (3) AlBashiti's acts affected interstate or foreign commerce.

9. Regarding Count Two of the Superseding Complaint (18 U.S.C. §2 and §1030(a)(5)), the United States must prove: (1) that AlBashiti knowingly conducted a transaction with one or more access devices that had been issued to another person; (2) that AlBashiti did so to obtain money, good or any thing of value of at least $1,000 during any one-year period; (3) that AlBashiti did so with the intent to defraud; and (4) AlBashiti's conduct affected interstate or foreign commerce. An access device means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

10. Regarding Count Three of the Superseding Indictment (18 U.S.C. §2 and §1030(a)(2)), the United States must prove (1) that AlBashiti knowingly used or trafficked in one or more unauthorized access devices; (2) that by such conduct AlBashiti obtained any money, good or thing of value with a total value of at least $1,000 during any one-year period; (3) that AlBashiti did so with intent to defraud; and (4) AlBashiti's conduct affected interstate or foreign commerce. An "access device" is a credit card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other means of account access that can be used alone or in conjunction with another access device, to get money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by a paper instrument). Passwords are access devices. An "unauthorized access device" is an access device that's lost, stolen, expired, canceled, revoked, or obtained with the intent to defraud. To "use" includes any effort to obtain money, goods, services, or any other thing of value, or to initiate a transfer of funds with an unauthorized access device. To "traffic in" means to transfer, or otherwise dispose of an unauthorized access device to another, or to possess or control an unauthorized device with the intent to transfer or dispose of it to another person. To act "with intent to defraud" means to act with the intent to deceive or cheat, usually for personal financial gain or to cause financial loss to someone else. The term "interstate commerce" refers to any transaction or event

that involves travel, trade, transportation or communication between a place in one state and a place in another state. The term "foreign commerce" refers to any transaction or event that involves travel, trade, transportation or communication between a place in the United States and a place outside the United States.

11. Counts Two and Three allege that AlBashiti also may be found guilty as an aider and abettor. Title 18, United States Code, Section 2, provides that whoever commands, procures, assists in, or causes the commission of a crime shall be held accountable and punished in the same manner as the principal, or the person who actually carried out the task. This means that AlBashiti 's guilt may be proven even if AlBashiti did not personally perform every act involved in the commission of the charged crime. The law recognizes that ordinarily, anything a person can do for herself may also be accomplished by directing another person as an agent, or by acting together with another person, or by acting under the direction of another person, or by acting together with another person or persons in a joint effort. So, if the acts or conduct of another person were willfully directed or authorized by AlBashiti, or if AlBashiti aided and abetted another person by willfully joining together with that person in the commission of a crime, then the law holds AlBashiti responsible for the conduct of that person, just as if AlBashiti had engaged in the conduct himself.

12. I have also included as part of **Exhibit C** the true and accurate text of 18 U.S.C. § 3282, which is the statute of limitations for the crimes charged in Count One

through Three of the Superseding Complaint. The statute of limitations requires that a defendant be formally charged within five years of the date on which the offense or offenses were committed.

13. I have thoroughly reviewed the applicable statute of limitations for the crimes charged in Count One through Three of the Superseding Complaint, and the prosecution of the charges in this case are not barred by the statute of limitations. Because the applicable statute of limitations is five years, an indictment or information needs to be returned by May 19, 2028.

14. The United States will prove its case against AlBashiti through witness testimony and documentary evidence.

15. AlBashiti has not been tried or convicted of any offense charged in the indictment, nor has he been ordered to serve any sentence in connection with this case.

SUMMARY OF THE INVESTIGATION AND FACTS OF THE CASE

16. A cybercriminal forum (the "Forum") known to U.S. law enforcement was a marketplace where individuals such as AlBashiti would promote and facilitate a wide variety of criminal activities including, among other activities, computer hacking, the sale of access to protected computers worldwide, and trafficking in stolen data, including personally identifiable information of U.S. residents. AlBashiti, using

the online moniker "r1z", offered numerous illegal services for sale on the Forum. On or about May 8, 2023, an FBI undercover employee (hereinafter "UC1") observed that AlBashiti was offering to sell access to 50 victim companies that were using one of two particular commercial firewall products.

17. On or about May 19, 2023 UC1 purchased from AlBashiti access to 50 victim companies that were using one of two commercial firewall protections. After making this purchase, AlBashiti sent UC1 a list of IP addresses and usernames, as well as instructions on how to use that information to gain access to the computer networks of the victim companies. U.S. law enforcement verified that the information AlBashiti provided UC1 enabled unauthorized access to the 50 victim companies' computer systems. Further, U.S. law enforcement confirmed with the companies that sell the commercial firewall products that the information sold by AlBashiti appeared to be malicious computer code designed to gain access to victim companies' computer systems using the respective firewall products.

18. Additionally, on or about September 18, 2023, UC1 and AlBashiti discussed the sale of malware that could turn off Endpoint Detection and Response (hereinafter "EDR"). EDR is used in cyber security to monitor, protect, and respond to malware and protect computer systems. AlBashiti informed UC1 that he had new malware that could disable EDR security products sold by three different companies. UC1 granted AlBashiti access to a computer server (the "FBI Server") to allow

AlBashiti to demonstrate that this malware would work. The FBI Server was protected by an EDR product. After being given access to the FBI Server, FBI personnel observed and recorded AlBashiti use his malware to disable the EDR protection on the FBI Server.

19. UC1 continued communication with AlBashiti through at least October 13, 2023 and purchased additional, highly effective malware capable of elevating internal user privileges without authorization.

20. During the course of the investigation, AlBashiti accessed the FBI Server from a particular IP address (hereinafter the "IP Address"). Additional investigation showed that the IP Address was used (1) to gain unlawful access to government computer systems belonging to a U.S. territory, and (2) during a ransomware attack against a U.S. manufacturing company in or around June 2023, resulting in estimated losses exceeding $50 million.

21. Investigation has also established that AlBashiti is the individual behind the r1z moniker. On or about October 20, 2016, AlBashiti applied to the United States Department of State for a visa to enter the United States. In connection with that application, AlBashiti used a particular Google email address (the "Email Account"). Law enforcement obtained records related to the Forum. These records show that the Email Account was used by r1z to create the account on the Forum.

22. The investigation further revealed that the Email Account is linked to a Google Pay Account with various names including "Firas.B", "Feras B," "Firas Bashiti," and "Firas K. Bashiti." Further, the Google Pay Account is linked to credit cards in the names of "Firas K. Bashiti" and "Firas Bashiti."

IDENTIFICATION

23. AlBashiti is a citizen of Jordan born on July 12, 1985. A photograph of him is attached as **Exhibit D**.

CONCLUSION

24. I request that any items relevant to the charged offenses found in the AlBashiti's possession at the time of his arrest be delivered to the United States, if the extradition is granted.

25. Should Georgian authorities require supplementary information in order to grant the extradition, I ask for a reasonable time to provide such information.

26. This affidavit was sworn to before a Magistrate Judge of the United States District Court for the District of New Jersey who is duly empowered to administer an oath for this purpose.

David E. Malagold
Assistant United States Attorney

Sworn to before me in Newark, New Jersey this 13th day of Decembre, 2023.

Honorable André M. Espinosa
United States Magistrate Judge

EXHIBIT LIST

EXHIBIT A	Certified Copy of Superseding Complaint
EXHIBIT B	Certified Copy of Arrest Warrant
EXHIBIT C	Relevant Legal Provisions
EXHIBIT D	Photograph

EXHIBIT A

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	TO BE FILED UNDER SEAL
	:	
v.	:	Hon. André M. Espinosa
	:	
FERAS KHALIL AHMAD ALBASHITI, a/k/a "r1z," a/k/a "Feras Bashiti," a/k/a "Firas Bashiti,"	:	Mag. No. 23-11200
	:	
	:	SUPERSEDING CRIMINAL COMPLAINT

I, Christopher Baker, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Task Force Officer with the Federal Bureau of Investigation, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

Continued on the attached pages and made a part hereof.

s/ Christopher Baker

Christopher Baker, Task Force Officer
Federal Bureau of Investigation

Task Force Officer attested to this Complaint by telephone pursuant to FRCP 4.1(b)(2)(A).

December 6, 2023 at
Newark, New Jersey

HONORABLE ANDRÉ M. ESPINOSA
UNITED STATES MAGISTRATE JUDGE

Signature of Judicial Officer

Signed by Task Force Officer Christopher Baker at Judge Espinosa's direction pursuant to F.R.C.P. 4.1(b)(6)(C).

ATTACHMENT A

COUNT ONE
(Fraud and Related Activity in Connection with Computers)

On or about May 19, 2023, in the District of New Jersey and elsewhere, the defendant,

FERAS KHALIL AHMAD ALBASHITI, a/k/a "r1z",

did knowingly and with intent to defraud traffic in any password and similar information through which a computer may be accessed without authorization, and such trafficking affected interstate and foreign commerce.

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

COUNT TWO
(Fraud and Related Activity in Connection with Access Devices)

On or about May 19, 2023, in the District of New Jersey and elsewhere, the defendant

FERAS KHALIL AHMAD ALBASHITI, a/k/a "r1z",

did knowingly and with intent to defraud effect transactions with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period, the aggregate value of which is equal to or greater than $1,000.

In violation of Title 18, United States Code, Section 1029(a)(5) and Section 2.

COUNT THREE
(Fraud and Related Activity in Connection with Access Devices)

On or about May 19, 2023, in the District of New Jersey and elsewhere, the defendant

FERAS KHALIL AHMAD ALBASHITI, a/k/a "r1z",

did knowingly and with intent to defraud traffic in and use one or more unauthorized access devices during any 1-year period, and by such conduct obtain anything of value aggregating $1,000 or more during that period.

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

ATTACHMENT B

I, Christopher Baker, am a Task Force Officer with the Federal Bureau of Investigation ("FBI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with witnesses and other law enforcement officers, and my review of reports, documents, and items of evidence. Where statements of others are related herein, they are related in substance and in part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

I. Background

At various times relevant to this Complaint:

1. The defendant, FERAS KHALIL AHMAD ALBASHITI, a/k/a "r1z", ("ALBASHITI") was a citizen of Jordan and resided in the Republic of Georgia.

2. An "access broker" was an individual who acquired and sold unlawful access to victim computer systems. Typically, access brokers sold this access to individuals committing various types of computer-related crimes, such as business email compromises, unlawful exfiltration of data, and ransomware attacks.

3. "Malware" referred to software programs designed to disrupt the intended operation of a computer or other device, gather sensitive information, gain access to the computer or other device, and take other unwanted actions.

4. A "firewall" was a computer network security system that monitored and controlled incoming and outgoing network traffic based on predetermined security rules.

5. "Penetration testing" or "pen testing" was a cyber security exercise where a user attempts to find and exploit potential vulnerabilities in a computer network.

6. "Endpoint Detection and Response" or "EDR" was used in the cyber security industry to monitor, detect, and respond to cyber threats such as ransomware and malware and to protect computer networks.

7. "Cybercrime Forums" were online forums where, either overtly through public messages or covertly through private messages, cybercriminals promoted and facilitated a wide variety of criminal activities including, among other activities, computer hacking and trafficking in stolen data.

II. The Forum and ALBASHITI's Sale of Malware

8. As part of an unrelated investigation, the FBI obtained records related to a particular Cybercrime Forum (the "Forum"). According to these records, a Forum user with the online moniker "r1z" registered an account on the Forum using a particular Google email address (the "Email Account") in or around 2018.

9. According to Forum records, on or about July 3, 2020, r1z and another Forum user communicated regarding mobile banking malware.

10. Beginning in May 2023, an FBI employee acting in an undercover capacity ("UC1") visited the Forum on multiple occasions and: (1) took screenshots of malware or other malicious code being offered for sale by r1z; and (2) purchased unauthorized access to victim computer networks from r1z.

11. For example, on or about May 8, 2023, UC1 visited the Forum and documented that r1z was offering to sell access to the computer networks of approximately 50 victim companies (the "Victim Companies") through the exploitation of two commercial firewall products sold by different companies ("Firewall-1" and "Firewall-2").

12. On or about May 16, 2023, r1z sold UC1 an unauthorized software modification of a commercially available penetration testing tool (the "Tool") over the Forum. Based on my training and experience and information learned during this investigation, the Tool (with the software modification) sold by r1z would enable a user to: (a) avoid paying a substantial licensing fee; (b) operate the Tool without notification to the owner of the legitimate version of the Tool; and (c) use the Tool to deploy malware on a victim computer network.

13. On or about May 19, 2023, UC1, who was at a location in New Jersey, initiated a private chat over the Forum with r1z regarding the purchase of access to the computer networks of Victim Companies using either Firewall-1 or Firewall-2.

14. During the May 19, 2023, communications, r1z provided UC1 a Bitcoin address for payment and r1z explained that UC1 would receive access to the Victim Companies approximately eight hours after payment. UC1 thereafter made a payment of approximately 0.19 BTC, which on May 19, 2023 was valued at over approximately $5,000.

15. After receiving payment, r1z explained to UC1 that r1z was working on UC1's order and stated that he would be providing access to 10 Victim Companies that were using Firewall-1 and 40 Victim Companies that were using Firewall-2.

16. Shortly thereafter, r1z sent UC1: (1) a link which contained a list of IP addresses and usernames associated with the Victim Companies; and (2) a link with

instructions on how to access the Victim Companies' computer networks using that information.

17. After receiving the above-referenced links from r1z, law enforcement verified that the information and instructions provided by r1z were effective in securing unauthorized access to all 50 Victim Companies' networks.

18. FBI personnel further confirmed with the companies that sell Firewall-1 and Firewall-2 that the information purchased from r1z appeared to be malicious code designed to provide unlawful access to victim computer networks through the disablement of Firewall-1 or Firewall-2.

19. On or about September 18, 2023, UC1 contacted r1z and inquired whether r1z was selling malware that could turn off EDR. In a private chat, r1z told UC1 that he possessed malware that could turn off EDR security products sold by three different companies (EDR Company-1, EDR Company-2, and EDR Company-3).

20. UC1 and r1z agreed on a price of $15,000 per EDR exploit. UC1 thereafter selected the exploit for EDR Company-1.

21. R1z asked UC1 to grant him access to a server in order to show proof that the malware would indeed turn off the EDR product sold by EDR Company-1. UC1 granted r1z access to a server controlled by the FBI (the "Server"), which recorded and monitored r1z's activity on the Server. The Server was equipped with EDR Company-1's EDR ("EDR1") just as if it were a private computer server operated by a potential victim.

22. R1z accessed the Server on or about September 20, 2023. FBI monitored this activity. While inside the Server, r1z executed a file named "r1z.exe", which rendered EDR1 nonfunctional. The file also launched a hidden task which created an entry point or "back door" access to the compromised system.

23. On several occasions while r1z was accessing the Server, FBI observed and recorded that r1z was using a particular IPv4 address (the "IP Address") to gain remote access to the Server.

24. On or about September 26, 2023, EDR Company-2 reported that the IP Address was actively downloading EDR Company-2's software from a government computer system belonging to a U.S. Territory. Law enforcement was thereafter able to capture multiple instances of malware being built and executed over the IP Address. Based on this investigation, law enforcement believes this malware was being tested to disable the EDR protection sold by EDR Company-2.

25. UC1 has continued communication with r1z regarding the purchase of additional malware through at least October 13, 2023. UC1 has further purchased

additional malware from r1z designed and capable of elevating internal user privilege and compromising victim servers. Expert analysis on this malware has revealed that the malware is novel and appears to be highly effective at compromising victim computer networks.

26. Additional investigation has also revealed that the IP Address was used in or around June 2023 during a ransomware attack against a U.S. manufacturing company, which caused estimated damages in excess of $50 million.

III. Identification of ALBASHITI

27. Through this investigation, law enforcement obtained United States Department of State records, which revealed that on or about October 20, 2016, ALBASHITI requested a visa from the United States State Department to enter the United States. In connection with that application, ALBASHITI used the Email Account to register with the State Department – the same email account used to register the r1z moniker on the Forum, as set forth above.

28. According to Google records, the Email Account was opened on or about December 15, 2009 with a subscriber name of "Firas K".

29. The investigation further revealed that the Email Account is linked to a Google Pay Account with various names including "Firas.B", "Feras B," "Firas Bashiti," and "Firas K. Bashiti." Further, the Google Pay Account is linked to credit cards in the names of "Firas K. Bashiti" and "Firas Bashiti."

EXHIBIT B

AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

District of New Jersey

United States of America
v.
FERAS KHALIL AHMAD ALBASHITI, a/k/a "r1z," a/k/a "Feras Bashiti," a/k/a "Firas Bashiti,"

Case No. 23-11200

Defendant

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay

(name of person to be arrested) FERAS KHALIL AHMAD ALBASHITI, a/k/a "r1z," a/k/a "Feras Bashiti," a/k/a "Firas Bashiti," ,

who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☑ Complaint

☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

18 U.S.C. § 1030(a)(6)(A) (Fraud and related activity in connection with computers)
18 U.S.C. § 1029(a)(5) (Fraud and related activity in connection with access devices)
18 U.S.C. § 1029(a)(2) (Fraud and related activity in connection with access devices)

Date: 12/06/2023

Issuing officer's signature

City and state: Newark, New Jersey

André M. Espinosa
Printed name and title

Return

This warrant was received on *(date)* _____, and the person was arrested on *(date)* _____
at *(city and state)* _____.

Date: _____

Arresting officer's signature

Printed name and title

This second page contains personal identifiers provided for law-enforcement use only and therefore should not be filed in court with the executed warrant unless under seal.

(Not for Public Disclosure)

Name of defendant/offender: FERAS KHALIL AHMAD ALBASHITI

Known aliases: r1z, Feras Bashiti, Firas Bashiti

Last known residence: Tiblisi, Georgia

Prior addresses to which defendant/offender may still have ties:
Nweral Housing, Aldalleh Circle Marj Alhamam, Amman, Jordan

Last known employment:

Last known telephone numbers:

Place of birth: Kuwait

Date of birth: 07/12/1985

Social Security number:

Height: Weight:

Sex: Race:

Hair: Eyes:

Scars, tattoos, other distinguishing marks:

History of violence, weapons, drug use:

Known family, friends, and other associates *(name, relation, address, phone number)*:

FBI number:

Complete description of auto:

Investigative agency and address: Federal Bureau of Investigation (Newark Office)
Attn: Task Force Officer Chistopher Baker

Name and telephone numbers (office and cell) of pretrial services or probation officer *(if applicable)*:

Date of last contact with pretrial services or probation officer *(if applicable)*:

EXHIBIT C

RELEVANT LEGAL PROVISIONS

Exhibit C contains the applicable portions of statutes describing the offenses with which FERAS KHALIL AHMAD ALBASHITI, also known as "r1z," "Feras Bashiti," and "Firas Bashiti," is charged, the penalties that he faces if convicted, and the applicable statutes of limitations. Ellipses are used to indicate the omission of portions of the statutes and asterisks are used to indicate the omission of paragraphs or sub-paragraphs of the statutes because those portions and paragraphs or sub-paragraphs do not apply to the cases against AlBashiti.

Title 18, United States Code, Section § 1030(a)(6)(A), (c)(2)(A) and (i)
Fraud and related activity in connection with computers

(a) Whoever— . . .
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--
(A) such trafficking affects interstate or foreign commerce;

(c) The punishment for an offense under subsection (a) or (b) of this section is--
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(i)
(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—
(A)such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and
(B)any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

* * *

Title 18, United States Code, Section § 1029(a)(2), (a)(5), and (c)(1)(A)
Fraud and related activity in connection with access devices

(a) Whoever— . . .
(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;. . .

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000

(c) Penalties.—
(1) Generally.--The punishment for an offense under subsection (a) of this section is--
(A) in the case of an offense that does not occur after a conviction for another offense under this section--
(i) if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both;
(ii) if the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

(C)in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

* * *

Title 18, United States Code, Section § 982
Criminal Forfeiture

(a)
(2) The court, in imposing sentence on a person convicted of a violation of, or a conspiracy to violate—

(B) section 471, 472, 473, 474, 476, 477, 478, 479, 480, 481, 485, 486, 487, 488, 501, 502, 510, 542, 545, 555, 842, 844, 1028, 1029, or 1030 of this title, shall order that the person forfeit to the United States any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of such violation.

* * *

Title 18, United States Code, Section 3282
Offenses not capital

(a) In General.–
Except as otherwise expressly provided by law, no person shall be prosecuted, tried, or punished for any offense, not capital, unless the indictment is found or the information is instituted within five years next after such offense shall have been committed.

* * *

EXHIBIT D