Department of Justice

STATEMENT OF

ANDREW LOURIE
ACTING PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL
AND CHIEF OF STAFF
CRIMINAL DIVISION
UNITED STATES DEPARTMENT OF JUSTICE

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON THE JUDICIARY
SUBCOMMITTEE ON CRIME,
TERRORISM, AND HOMELAND SECURITY

CONCERNING

"PRIVACY AND CYBERCRIME ENFORCEMENT ACT OF 2007""

PRESENTED

DECEMBER 18, 2007

Statement of

Andrew Lourie

Acting Principal Deputy Assistant Attorney General
and Chief of Staff
Criminal Division
United States Department of Justice

Before the Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
United States House of Representatives

December 18, 2007

Good morning, Chairman Scott and Ranking Member Gohmert. It is a pleasure to appear before you today to testify about the Department of Justice's commitment to combating computer crime and identity theft, and about the important legislation this Committee is considering to address these crime threats.

I. THE THREAT OF COMPUTER CRIME AND IDENTITY THEFT

As information technology increasingly pervades every aspect of our society, the opportunities for criminals to take advantage of it has commensurately increased. One of the most significant harms of this criminal exploitation of computers and computer networks has been the rise of identity theft. Identity theft is pervasive throughout the United States and around the world. Every day criminals hunt for our personal and financial data so that they can use the data to commit fraud or sell the data to other criminals.

As the President's Identity Theft Task Force recently stated in its Strategic Plan, identity theft "exacts a serious toll on the American public," with annual monetary losses "in the billions of dollars."[1] The harm of identity theft, however, extends well beyond direct financial losses to victims. Businesses must bear indirect costs of fraud prevention and mitigation of the harm once it has occurred, individual victims often suffer indirect financial costs (such as costs incurred in civil litigation by creditors), and some victims spend substantial amounts of time to repair the damage that the identity thieves caused.

Furthermore, many identity-theft victims report that they must bear the uncertainty of whether and how an identity thief will cause new problems for them. As one victim put it, in connection with the recent sentencing of an identity thief,

> I am constantly wondering when I will be attacked again. I have no way of knowing who else [the defendant] has distributed my personal information to . . . . It would have been better to have been mugged at gunpoint, since at least then I would have my peace of mind knowing that it was a one-time event.[2]

Today, criminals are able to obtain personal information nearly everywhere it is located or stored. Hackers have developed tools to penetrate firewalls, use automated processes to search for account data or other personal information, export the data, and hide their tracks. According to the Secret Service, many major breaches in credit card systems in 2006 originated outside the United States, and criminals operating in those two countries have been directly involved in some of the largest breaches of U.S. financial systems over the past five years.[3]

---

[1] PRESIDENT'S IDENTITY THEFT TASK FORCE, COMBATING IDENTITY THEFT: A STRATEGIC PLAN at 11 (April 2007), *available at* http://www.idtheft.gov/.
[2] *See* United States Attorney's Office, Western District of Washington, Press Release (May 4, 2007), *available at* http://seattle.fbi.gov/dojpressrel/2007/pr050407.htm.
[3] PRESIDENT'S IDENTITY THEFT TASK FORCE, *supra*, at 15.

"Phishing" is another prevalent attack that has caused massive losses to consumers and businesses. Phishers send emails that appear to be coming from legitimate, well-known sources – often, financial institutions or government agencies – effectively stealing the identities of these entities. In one example, these email messages tell recipients to verify personal information or risk cancellation of their accounts. The emails provide a website to enter the information, but when the user clicks on the link, it leads to a web site that appears legitimate but is in fact controlled by the phishers. The user then enters personal identifying information, such as name, address, account number, PIN, and social security number. Phishers harvest this information and use it to commit fraud or sell it to other criminals.

The Strategic Plan of the President's Identity Theft Task Force provides considerable detail about the many ways that criminals perpetrate identity theft and about the ways in which the Federal Government can address this growing threat. The Identity Theft Task Force, which the President established in May 2006, was charged with producing a coordinated strategic plan to further improve the effectiveness and efficiency of the federal government's activities in the areas of identity theft awareness, prevention, detection, and prosecution. Released in April, 2007, this comprehensive strategy focuses on improvements in four key areas: (1) keeping sensitive consumer data out of the hands of identity thieves through better data security and more accessible education; (2) making it more difficult for identity thieves who obtain consumer data to use it to steal identities; (3) assisting the victims of identity theft in recovering from the crime; and (4) deterring identity theft by more aggressive prosecution and punishment of those who commit the crime. These themes are consonant with the legislation that the Committee is currently considering. The Department was pleased to recognize how much common ground we share and would commend the Strategic Plan to the members of this committee as an invaluable resource.

II. THE ROLE OF LAW ENFORCEMENT

A. Collecting Information and Receiving Complaints

Currently, federal law enforcement has a number of sources of information about cybercrime and identity theft. For example, the FBI and the National White Collar Crime Center (NWC3) have developed an online complaint mechanism for citizens to report internet-related fraud and other crimes. The Internet Crime Complaint Center (IC3) provides an easy way for computer users across the country and around the world to make these reports. The IC3 currently receives more than 20,000 complaints per month from victims of online crime. Moreover, it provides an important means of analyzing these reports and disseminating that information as case leads to the right law enforcement agency.

In addition, in order to respond to the challenges of multinational Internet fraud, and to enhance consumer protection and consumer confidence in e-commerce, thirteen countries instituted *econsumer.gov*, a joint effort to gather and share cross-border e-commerce complaints. The project has two components: a multilingual public Web site, and a government, password-protected Web site. The public site provides general information about consumer protection in all countries that belong to the ICPEN (International Consumer Protection Enforcement Network), contact information for consumer protection authorities in those countries, and an online complaint form. All information is available in English, French, German, and Spanish. Using the existing Consumer Sentinel network (a database of consumer complaint data and other investigative information operated by the U.S. Federal Trade Commission), the incoming complaints are shared with participating law enforcement agencies, such as the FBI.

B. Promoting Public/Private Partnerships

Private sector entities – including the financial services industry and credit reporting agencies – also are important sources of information for law enforcement agencies. They often are best positioned to identify anomalies that are indicative of identity theft and generally are the first to become aware of intrusions into their computer networks. For this reason and others, federal law enforcement has undertaken numerous public- and private-sector collaborations in recent years to improve information sharing.

For example, corporations have placed analysts and investigators with the IC3 to support its initiatives and investigations. The IC3 has also spun off an organization known as the Cyber Initiative and Resource Fusion Unit (CIRFU). The CIRFU combines resources from law enforcement with those of critical industry partners to identify trends in internet crime, develop enforcement initiatives, and alert consumers to problems, including identity theft scams.

In addition, the United States Secret Service leads Electronic Crimes Task Forces that focus on computer- and identity theft-related crimes. Inaugurated in 2001, the twenty-four task forces include industry and other private sector members. They provide an important forum for the sharing of threat and trend information and for the reporting of cybercrimes.

Finally, InfraGard is a national information sharing network between the FBI and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants. Its goals include increasing the level of information sharing and reporting between InfraGard members and the FBI on a variety of cybercrime matters, including identity theft.

C. Prosecuting Computer Crime and Identity Theft

For some time, the Department of Justice has been deeply committed to aggressively pursuing all forms of cybercrime and identity theft. Through interagency task forces and individual investigations, federal prosecutors have been prosecuting significant cases of identity theft. The following are examples of these prosecutions across the country:

> ***Virginia****:* On February 9, 2007, in the Eastern District of Virginia, a defendant was sentenced to 94 months in federal prison for aggravated identity theft, access device fraud, and conspiracy to commit bank fraud. The defendant, who went by the Internet nickname "John Dillinger," was involved in extensive illegal online "carding" activities. He received e-mails or instant messages containing hundreds of stolen credit card numbers – usually obtained through phishing schemes or network intrusions – from "vendors" located in Russia and Romania. In his role as a "cashier" of these stolen credit card numbers, the defendant would electronically encode these numbers onto plastic bank cards, make ATM withdrawals, and return a portion to the vendors. Computers seized from the defendant revealed more than 4,300 compromised account numbers and full identity information (i.e., name, address, date of birth, social security number, mother's maiden name, etc.) for over 1,600 individual victims.[10]
>
> ***California****:* On January 16, 2007, in the Central District of California, a defendant was convicted of violating the CAN-SPAM Act of 2003, as well as other counts including aggravated identity theft and wire fraud. The defendant

[10]*See* U.S. Attorney's Office, Eastern District of Virginia, Press Release (February 9, 2007), *available at* http://www.usdoj.gov/usao/vae/Pressreleases/02-FebruaryPDFArchive/07/20070209robertsnr.pdf

operated a sophisticated "phishing" scheme in which he sent thousands of e-mails to America Online users that appeared to be from AOL's billing department. His e-mails urged AOL customers to "update" their AOL billing information or lose service and referred customers to one of several web pages, where they could input their personal and credit information. The defendant actually controlled those webpages. Using information he collected from the AOL customers, he then made unauthorized charges on the AOL customers' credit or debit cards. On June 14, 2007, the defendant was sentenced to six years in prison and ordered to pay over $1 million in restitution to his victims.[12]

Washington: On August 25, 2007, in the Western District of Washington, a man was sentenced to 37 months in prison for creating a botnet – a network of compromised computers that he could control – and using it to commit over $100,000 in fraud. In addition to this harm, however, the malicious code used to create the botnet caused damage to many computers across the Internet. These disruptions affected a Seattle hospital's computer systems in serious ways: doors to the operating rooms did not open, pagers did not work, and computers in the intensive care unit shut down. Luckily, no one was hurt because the hospital was able to switch to back up systems. The defendant accepted responsibility for over $250,000 worth of damage.[4]

In addition, a number of U.S. investigations have resulted in successful prosecutions in foreign countries. For example, based on close cooperation between the

[12] *See* U.S. Attorney's Office, Central District of California, Press Release (January 16, 2007), *available at* http://www.usdoj.gov/usao/cac/news/pr2007/079.html

[4] *See* U.S. Attorney's Office, Western District of Washington, Press Release (August 25, 2006), *available at* http://www.usdoj.gov/usao/waw/press/2006/aug/maxwell.html.

Department, the FBI legal attaché, and Romanian authorities, Prosecutors from the Romanian Directorate for Investigating Organized Crime and Terrorism arrested 9 Romanian citizens on fraud and identity theft charges on November 13, 2007. These Romanians were part of a criminal organization that specialized in "phishing" information from computer users, imprinting credit and debit card information onto counterfeit cards, and obtaining cash from ATM machines and Western Union locations. Romanian police officers executed 21 simultaneous search warrants and seized computers, card reading and writing devices, blank cards, and other equipment. Initial loss estimates total more that $130,000.[5]

These prosecutions both at home and abroad properly punish offenders for the harms they cause. Successful prosecutions such as these will also generate a significant deterrent effect, an important part of addressing the overall cybercrime problem.

III. THE PRIVACY AND CYBERCRIME ACT OF 2007 (H.R. 4175)

While law enforcement is taking many steps to aggressively address the threat of cybercrime and identity theft, loopholes and shortcomings in existing law have inhibited its ability to do so. The Privacy and Cybercrime Act of 2007 would address several of these shortcomings and provide important tools to promote law enforcement's efforts.

In particular, the Department applauds the amendments in section 108 of the Act that would assure that victims of identity theft receive fair restitution for the time spent to remediate the harm resulting from identity theft offenses. Similarly, the Department supports the inclusion of section 103 which would enhance our ability to prosecute criminals who steal sensitive information from computers, section 104 (with some technical amendments that I will describe later) that would close loopholes in the cyber-extortion statute, and sections 101 and 105 that would enhance our ability to bring

[5] *See* Department of Justice, Press Release (November 13, 2007), *available at* http://www.cybercrime.gov/romanianphishingArrest.htm

computer crime charges against criminal conspiracies and organized criminal groups. In addition to these many positive aspects, the Department would like to provide some additional proposals that would strengthen the bill. The Department would also like to recommend a number of technical suggestions for Title I of the Act.

A. Additional Provisions That Would Strengthen the Act

1) Malicious Spyware, Botnets, and Keyloggers

The Department strongly encourages the Committee to consider adding to the bill an amendment to 18 U.S.C. § 1030(a)(5) that would appropriately penalize the use of malicious spyware, botnets, and keyloggers. Criminals routinely use these tools to steal sensitive information and commit identity theft and other crimes, and federal law creates a loophole that significantly inhibits the prosecution of such offenders.

Existing section 1030(a)(5) criminalizes actions that cause "damage" to computers, i.e., that impair the "integrity or availability" of data or computer systems. Absent special circumstances, the loss caused by the criminal conduct must exceed $5,000 to constitute a federal crime. Many identity thieves obtain personal information by installing "bots" and malicious spyware on numerous individual computers. Whether or not the programs succeed in obtaining the unsuspecting computer owner's financial data, these sorts of programs harm the "integrity" of the computer and data. Nevertheless, it is often difficult or impossible to measure the loss this damage causes to each computer owner, or to prove that the total value of these many small losses exceeds $5,000.

Two amendments could remedy this situation, and Congress could enact them separately or in tandem. First, Congress could amend section 1030(a)(5) to make it a misdemeanor offense where a person damages protected computers but causes less than $5,000 in loss. The current felony penalty would remain for losses that exceed $5,000.

Second, Congress could create an alternative basis for triggering the existing felony provision: damage to more than 10 protected computers. In either case, the government would have another tool for prosecuting individuals who plant malicious spyware on a large number of computers.

We note that S. 2168, as passed by the Senate on November 15, 2007, as well as the Identity Theft Task Force Report, contains language that accomplishes both of these goals. We urge Congress to add these provisions to H.R. 4175 as it would close a significant gap in the computer fraud and identity theft regime. Moreover, even if Congress decides to enact section 106 without amendment, we urge it to add a provision that would amend existing section 1030(a)(5) to include "***damage affecting ten or more protected computers during any one-year period***."

2) Enhancing the Prosecution of Identity Theft

The current identity theft offense (18 U.S.C. § 1028(a)(7)) and the aggravated identity theft offense (18 U.S.C. § 1028A) are both limited to stealing the identity of an individual and do not specifically address the misuses of the identification of a corporation or organization. The Department recommends adding a provision that would amend both statutes to ensure that identity thieves who steal identity information belonging to corporations and organizations can be prosecuted, such as when they send phishing emails using the entity's name, logo, and other identifying marks in order to trick the end user. The legislation should also add several new crimes to the list of aggravated identity theft offenses to ensure that the aggravated identity theft offense can be applied to a wider range of federal crimes that are frequently associated with identity theft, such as mail theft. This amendment was proposed in the Identity Theft Task Force's Strategic Plan, and S. 2168 contains such a provision. Proposed language for this amendment is contained in Appendix A.

B. Amendments to the Provisions of H.R. 4175

1) Section 102 – Law Enforcement Notification of Security Breaches Involving Sensitive Personally Identifiable Information

Section 102(c)(2) of the Act requires that "[t]he Secret Service and the Federal Bureau of Investigation shall annually publish in the Federal Register a list of all notifications submitted the previous calendar year and the identity of each entity with respect to which the major security breach occurred." Because of the potential national security implications of many security breaches, the Act should waive the publication requirement in some circumstances. We note the bill does later establish a waiver for national security reasons in section 203, but that waiver applies only to the portion of the bill addressing 5 U.S.C. § 553a, and would not affect the publication requirement. A similar national security waiver should be available in Section 102. We look forward to the opportunity to work with the Committee to address this issue.

Section 102(e)(3)(A)(i) of the bill also defines the term "major security breach" to include any security breach whereby the "means of identification pertaining to 10,000 or more individuals" is lost. This threshold is too high. To give the number some context, an intrusion attack involving the theft of as few as 1,000 credit card numbers is, under the current United States Sentencing Guidelines, presumed to involve a minimum loss of $500,000. Similarly, law enforcement should be fully empowered to open an investigation, for example, where the breach involves the records of "only" 9,000 individuals. We therefore recommend that this number be reduced to 1,000. Furthermore, the use of these thresholds could result in failure to report in critical situations that do not involve large numbers. For that reason, we believe that this section should be amended to also require notification where there may be a threat to national security or a risk of significant monetary loss, without regard to the number of records breached.

2) Section 104 – Cyber-Extortion

This provision would add the words "or to access without authorization or exceed authorized access to a protected computer" to 18 U.S.C. § 1030(a)(7). If the goal is to take into account the problem that some cyber-criminals extort companies without explicitly threatening to cause damage to computers, then we recommend a slightly different solution to that problem.

More importantly, section 104 would not cover several emerging types of criminality. For example, the language would not cover the situation in which a criminal has *already* stolen the information and then threatens to disclose it unless paid off. Similarly, other criminals cause damage first – such as by accessing a corporate computer without authority and encrypting critical data – and then threaten that they will not correct the problem unless the victim pays.

In order to address these situations, the Department recommends amending section 104 of the bill so that it matches section 6 of S. 2168, which passed the Senate on November 15, 2007. (The proposal also appeared in the Identity Theft Task Force's Strategic Plan.) That text is provided in Appendix B for your convenience.

3) Section 106 – Penalties for Section 1030 Violations

We support the addition of forfeiture provisions for 18 U.S.C. § 1030. The wording in the current bill, however, does not adequately accomplish its goal because it does not specify what procedures will be used in forfeiture hearings. Thus, instead of the wording in section 106 of the bill, however, we would propose new language to be placed in two new subsections (*See* Appendix C). This new language is necessary for several reasons.

First, the law should allow for both civil and criminal forfeiture. Second, like other forfeiture provisions, the forfeiture of property used to facilitate computer crimes should also include real property.

Third, the following procedural reference should be included for the civil provisions of Chapter 46 of Title 18 at the end of subsection (j):

> *Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) of title 18 shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security.*

This change would take into account the fact that the Homeland Security Act moved certain enforcement officials from the Treasury Department to the Department of Homeland Security. It would also harmonize this section with existing forfeiture law and save limited judicial and prosecutorial resources in uncontested civil forfeiture cases.

Finally, any references to "proceeds" in the forfeiture section should be changed to "gross proceeds." Failure to include the phrase "gross proceeds" will allow criminals to argue that they are entitled to deduct their overhead expenses and costs-of-doing-business from the amounts the government attempts to recover via forfeiture. Criminals should not be allowed such a loophole.

4) Section 107 – Additional Funding

Consistent with the Department's budgetary requests, we support the proposal to give additional funds to various law enforcement agencies to investigate and prosecute criminal activity involving "computers and other information technology." Since almost any crime today uses computers or telephones, however, this broad language would not necessarily target the crimes upon which this bill focuses. Instead, we would suggest that the funds be allocated to "investigate and prosecute criminal activity involving

unauthorized access to computers, identity theft, and similar offenses." This would limit the distribution of the additional funding to combating the types of activity addressed by other sections of the Act.

In addition, we recommend that the Attorney General have authority to decide how best to allocate these funds within the Department. Thus, we propose striking the words "for the Criminal Division of the Department of Justice."

5) Section 109 – Review and Amendment of Federal Sentencing Guidelines

Section 109 provides a useful directive to the Sentencing Commission to reassess the sentencing of cyber-criminals. We support this provision, but would propose adding some additional criteria that the Commission should take into account in its revision of the Guidelines. Many of these additional factors appear in S. 2168, as passed by the Senate on November 15, 2007.

Intent to Cause Harm. Like the current statutory sentencing scheme, 18 U.S.C. § 1030(c)(3)(B) and (c)(4), the Guidelines explicitly address the question of intent to cause damage to computers. If the offender causes damage intentionally, the Guidelines call for a 4-level increase. U.S.S.G. §2B1.1(b)(14). Unfortunately, Subsection 14 contains a number of bases for an increased sentence, and this mix of factors does not always lead to the appropriate outcome. The source of this problem is the subsection's directive to "Apply the Greatest" of three elements, each of which should be treated separately in most cases. For example, the first of these elements directs the court to increase a defendant's guideline range by two levels if the offense includes the unauthorized access to a military computer or the theft of personal information. If the offender also intentionally causes damage, however, he triggers the second element, a 4-level increase, and the court will ignore the first element. Thus, if the offender intentionally damages a Pentagon computer, the Guidelines would assign him the exact same guideline range as

someone who intentionally damages a grocery store computer. This outcome makes little sense, and the Sentencing Commission should allow each of these elements to apply independently of one another. The bill could add as a criteria for the Commission, "*whether the defendant's intent to cause damage or intent to obtain personal information should be disaggregated and considered separately from the other factors set forth in USSG 2B1.1(b)(14).*"

Definition of "Victim." While the definition of victim appropriately includes those that suffer financially, it does not similarly take into account victims who suffer non-financial harm. U.S.S.G. §2B1.1, Application Note 1, restricts the definition of "victim" to include only those who have suffered loss that can be measured in monetary terms. This is inappropriate and should be corrected.

For example, the Guidelines provide for increases where a crime causes harm to many victims, yet this basic principle does not apply to victims whose privacy has been invaded. Thus, if a malicious spyware program invades the privacy of many computer owners but does not cause any quantifiable monetary loss, the sentencing increases set out in the Guidelines for crimes involving multiple victims do not apply. Yet it makes no sense for the guidelines to direct courts to enhance sentences for privacy invasions but then define "victim" to be only those that suffer monetary harm. The Sentencing Commission should address this problem by amending the definition of victim so that it includes persons whose privacy was invaded by the criminal offense. We suggest that the Commission be directed to evaluate "*whether the term 'victim' as used in USSG 2B1.1 should include individuals whose privacy was violated as a result of the offense in addition to individuals who suffered monetary harm as a result of the offense."*

Disclosure of Personal Information to Others. The Guidelines do not explicitly address the situation in which private information is disclosed to others beyond the individual who gains unauthorized access to it. Because posting stolen information on

the Internet or selling sensitive information to identity thieves increases the significance of the privacy invasion, the Sentencing Commission should amend the Guidelines to include an increased penalty for such an action, by considering "*whether the defendant disclosed personal information obtained during the commission of the offense.*"

Value of Information Stolen. In general, the market value of real-world stolen property is a good measure of the significance of the crime and the Guidelines appropriately increase sentences based on that value. The theft of electronic information, however, differs in one significant respect: the offender generally only *copies* the data and does not deprive the owner of possession or use of it. While this circumstance will reduce the harm experienced by the victim, the value of the information remains a good proxy for the significance of the offense.

In the case of computer data, moreover, it may prove difficult at times to establish the value of the information. Some types of information, such as a customer list, have a market value that can be established at trial through expert testimony or by introducing evidence that the offender sold it to another person. But it may be impossible to put a price tag on other types of information, even though it plainly cost someone a considerable amount of money to create the data. For example, an individual broke into a NASA computer in 1999 and stole a software program developed to control the physical environment on the International Space Station. It cost NASA $1.7 million dollars to develop this software, but it may or may not have value on the open market. In these situations, the cost of developing the information, or the harm caused by disclosing it, provides a reasonable alternative measure of its value, and courts should be able to utilize these measures in calculating the harm caused by the offense. We suggest that the bill direct the Commission to consider:

> *The potential and actual loss resulting from the offense, including the value of information obtained from a protected computer, regardless of whether the owner was deprived of use of the information, and considering such factors as the*

market value of the information, the cost of developing the information, the value to the owner of the information remaining confidential, and the harm caused by the disclosure of the information.[6]

* * *

In conclusion, the Department would like to emphasize that law enforcement has a critical role in addressing the growing threat of computer crime and identity theft. But we can do that only if we have the proper laws in place to investigate and prosecute these criminals and only if we have appropriate resources. The Privacy and Cybercrime Act of 2007 addresses many of those needs by closing loopholes in existing cybercrime statutes, improving our ability to prosecute criminal groups, and providing much-needed resources. With the changes I've suggested, the Act will be an important milestone in the fight against cybercrime.

Mr. Chairman, this concludes my remarks. I would be pleased to answer questions from you and other members of the Committee.

[6] We note that section 10(b)(3)(B) of S. 2168 contains similar language, but it focuses on the cost incurred by the victim. We believe that it is better to direct the U.S. Sentencing Commission to consider other factors as well, such as the harm caused by disclosure and the value of keeping the information confidential, in drafting an appropriate amendment to the U.S. Sentencing Guidelines.

APPENDIX A

PROPOSED AMENDMENTS TO THE IDENTITY THEFT AND AGGRAVATED IDENTITY THEFT STATUTES

Proposed Amendment to Aggravated Identity Theft Statute to Add Predicate Offenses

Congress should amend the aggravated identity theft offense (18 U.S.C. § 1028A) to include other federal offenses that recur in various identity-theft and fraud cases, specifically, mail theft (18 U.S.C. § 1708), uttering counterfeit securities (18 U.S.C. § 513), and tax fraud (26 U.S.C. §§ 7201, 7206, and 7207), as well as conspiracy to commit specified felonies already listed in section 1028A—in the statutory list of predicate offenses for that offense (18 U.S.C. § 1028A(c)).

Proposed Additions to Both Statutes to Include Misuse of Identifying Information of Organizations

(a) Section 1028(a) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

Section 1028A(a) of Title 18, United States Code, is amended by inserting in paragraph (1) the phrase "(including an organization as defined in Section 18 of this Title)" after the word "person".

(b) Section 1028(d)(7) of Title 18, United States Code, is amended by inserting in paragraph (7) the phrase "or other person" after the word "individual".

APPENDIX B

PROPOSED AMENDMENTS TO 18 U.S.C. § 1030(a)(7) (CYBER-EXTORTION)

Section 1030(a)

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any—

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

APPENDIX C

PROPOSED AMENDMENT TO 18 U.S.C. § 1030 (FORFEITURE)

18 U.S.C. § 1030

(i) Criminal Forfeiture

(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 property, real or personal, 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 gross proceeds that such person obtained, directly or indirectly, as a result of such violation;

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) Civil Forfeiture

(1) The following shall be subject to forfeiture to the United States and no property right shall exist in them:

(A) any property, real or personal, used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section; and

(B) any property, real or personal, which constitutes or is derived from gross proceeds traceable to any violation of this section, or a conspiracy to violate this section.

(2) Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) of

title 18 shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security.