APPENDIX F

Text of Amendment to 18 U.S.C. § 1030(a)(2)

The basis for this proposed amendment is set forth in Section III.D.4.b of the strategic plan, which describes gaps in the computer-related identity theft statutes.

Proposed Language:

1030(a) Whoever—

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains–

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer ~~if the conduct involved an interstate or foreign communication~~;

APPENDIX G

Text of Amendments to 18 U.S.C. §§ 1030(a)(5), (c), and (g), and to 18 U.S.C. § 2332b

The basis for these proposed amendments is set forth in Section III.D.4.b of the strategic plan, which describes gaps in the computer-related identity theft statutes.

Proposed Language:

18 U.S.C. § 1030

(a) Whoever—

(5)

(A) ~~(i)~~ knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) ~~(ii)~~ intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) ~~(iii)~~ intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; ~~and~~

~~(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—~~

~~(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;~~

~~(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;~~

~~(iii) physical injury to any person;~~

~~(iv) a threat to public health or safety; or~~

~~(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;~~

(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), ~~(a)(5)(A)(iii)~~, 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;

(3) ...(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), ~~(a)(5)(A)(iii)~~, or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

~~(4) (A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;~~

~~(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;~~

~~(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and~~

~~(5) (A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and~~

~~(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.~~

(4) (A) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety;

(v) damage affecting a computer used by or for a government entity in furtherance of the administration of justice, national defense, or national security; or

(vi) damage affecting ten or more protected computers during any 1-year period;

or an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (c)(4)(D) and (c)(4)(E), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subparagraphs (c)(4)(A)(i) through (vi), or an attempt to commit an offense punishable under this subparagraph;

(C) a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5) that occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(D) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title or imprisonment for not more than 20 years, or both;

(E) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title or imprisonment for any term of years or for life, or both; or

(F) a fine under this title, imprisonment for not more than one year, or both, for any other offense under subsection (a)(5), or an attempt to commit an offense punishable under this subparagraph.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) ~~of subsection (a)(5)(B)~~ ***subparagraph (c)(4)(A)***. Damages for a violation involving only conduct described in ~~subsection (a)(5)(B)(i)~~ ***subparagraph (c)(4)(A)(i)*** are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 2332b(g)(5)(B)(I)

...1030(a)(5)(A)~~(i)~~ resulting in damage as defined in ~~1030(a)(5)(B)(ii) through (v)~~ ***1030(c)(4)(A)(ii) through (vi)*** (relating to protection of computers)...

APPENDIX H

Text of Amendments to 18 U.S.C. § 1030(a)(7)

The basis for this proposed amendment is set forth in Section III.D.4.c of the strategic plan, which describes gaps in the cyber-extortion statute.

Proposed Language:

18 U.S.C. § 1030(a)(7)

(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 I

Text of Amendment to United States Sentencing Guideline § 2B1.1

The basis for this proposed amendment is set forth in Section III.D.4.d of the strategic plan, which describes the Sentencing Guidelines provision governing identity theft.

Proposed language for United States Sentencing Guidelines § 2B1.1, comment.(n.1):

"Victim" means (A) any person who sustained any harm, whether monetary or non-monetary, as a result of the offense. Harm is intended to be an inclusive term, and includes bodily injury, non-monetary loss such as the theft of a means of identification, invasion of privacy, reputational damage, and inconvenience. "Person" includes individuals, corporations, companies, associations, firms, partnerships, societies, and joint stock companies.

APPENDIX J

Description of Proposed Surveys

In order to expand law enforcement knowledge of the identity theft response and prevention activities of state and local police, the Bureau of Justice Statistics (BJS) should undertake new data collections in three areas: (1) a survey of law enforcement agencies focused on the response to identity theft; (2) enhancements to the existing Law Enforcement Management and Administrative Statistics (LEMAS) survey platform; and (3) enhancements to the existing training academy survey platform. Specifically, BJS should undertake to do the following:

- **New survey of state and local law enforcement agencies.** A new study focused on state and local law enforcement responses to identity theft should seek to document agency personnel, operations, workload, and policies and programs related to the handling of this crime. Detail on the organizational structure, if any, associated with identity theft response should be included (for example, the use of special units devoted to identity theft). The study should inquire about participation in regional identity theft task forces, community outreach and education efforts, as well as identity theft prevention programs. Information collected should also include several summary measures of identity theft in the agencies' jurisdictions (offenses known, arrests, referrals, outcomes), with the goal of producing some standardized metrics with which to compare jurisdictions.
- **Enhancement to existing LEMAS survey.** BJS should develop a special battery of questions for the existing LEMAS survey platform. The LEMAS survey, conducted roughly every three years since 1987, collects detailed administrative information from a nationally representative sample of about 3,000 agencies. The sample includes all agencies with 100 or more officers, and a stratified random sample of smaller agencies as well as campus law enforcement agencies. Information collected should include whether agencies presently enforce identity theft laws, utilize special units, have designated personnel, participate in regional identity theft task forces, and have policies and procedures in place related to the processing of identity theft incidents. The survey should also inquire whether agencies collect summary measures of identity theft in their jurisdictions, including offenses known, arrests, referrals, and any outcome measures. Finally, this study should also collect information on whether agencies are engaged in community outreach, education, and prevention activities related to identity theft.
- **Enhancement to existing law enforcement training academy survey.** BJS should develop a special battery of questions for the existing law enforcement training academy survey platform. A section of the data collection instrument should be devoted to the types of training, if any,

being provided by basic academies across the country in the area of identity theft. BJS should subsequently provide statistics on the number of recruits who receive training on identity theft, as well as the nature and content of the training. In-service training provided to active-duty officers should also be covered.

- **The Bureau of Justice Statistics should revise both the State Court Processing Statistics (SCPS) and National Judicial Reporting Program (NJRP) programs so that they are capable of distinguishing identity theft from other felony offenses.** In addition, the scope of these surveys should be expanded to include misdemeanor identity theft offenders. If SCPS and NJRP were able to follow identity theft offenders, then a variety of different types of court-specific information could be collected. These include how many offenders are charged with identity theft in the Nation's courts, what percentage of these offenders are released at pretrial, and how are the courts adjudicating (e.g., convicting or dismissing) identity theft offenders. Among those convicted identity theft offenders, data should be collected on how many are being sentenced to prison, jail, or probation. These projects should also illuminate the prior criminal histories or rap sheets of identity theft offenders. Both projects should also allow for the post conviction tracking of identity theft offenders for the purposes of examining their overall recidivism rates.
- BJS should ensure that other state court studies that it funds are reconfigured to analyze the problem of identity theft. For example, State Court Organization (SCO) currently surveys the organizational structure of the Nation's state courts. This survey could be supplemented with additional questionnaires that measure whether special courts similar to gun, drug, or domestic violence courts are being created for identity theft offenders. Also, SCO should examine whether courts are training or funding staff equipped to handle identity theft offenders.
- BJS should ensure that the Civil Justice Survey of State Courts, which examines civil trial litigation in a sample of the Nation's state courts, is broadened to identify and track various civil enforcement procedures and their utilization against identity thieves.

ENDNOTES

1. Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998). The Identity Theft Assumption and Deterrence Act provides an expansive definition of identity theft. It includes the misuse of any identifying information, which could include name, SSN, account number, password, or other information linked to an individual, to commit a violation of federal or state law. The definition thus covers misuse of existing accounts as well as creation of new accounts.

2. The federal financial regulatory agencies include the banking and securities regulators, namely, the Federal Deposit Insurance Corporation, the Federal Reserve Board, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Commodity Futures Trading Commission, and the Securities and Exchange Commission.

3. The public comments are available at ***www.idtheft.gov.***

4. Testimony of John M. Harrison, June 19, 2003, Senate Banking Committee, "The Growing Problem of Identity Theft and its Relationship to the Fair Credit Reporting Act."

5. *See* U.S. Attorney's Office, Western District of Michigan, Press Release (July 5, 2006), available at ***http://www.usdoj.gov/usao/miw/press/JMiller_Others10172006.html***.

6. Javelin Strategy and Research, *2007 Identity Fraud Survey Report: Identity Fraud is Dropping, Continued Vigilance Necessary* (Feb 2007), summary available at ***http://www.javelinstrategy.com***; Bureau of Justice Statistics (DOJ) (2004), available at ***http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf***; Gartner, Inc. (2003), available at ***http://www.gartner.com/5_about/press_releases/pr21july2003a.jsp***; FTC 2003 Survey Report (2003), available at ***http://www.consumer.gov/idtheft/pdf/synovate_report.pdf***.

7. *See* Business Software Alliance, *Consumer Confidence in Online Shopping Buoyed by Security Software Protection, BSA Survey Suggests* (Jan. 12, 2006), available at ***http://www.bsacybersafety.com/news/2005-Online-Shopping-Confidence.cfm***.

8. *See* Cyber Security Industry Alliance, *Internet Security Voter Survey* (June 2005) at 9, available at ***https://www.csialliance.org/publications/surveys_and_polls/CSIA_Internet_Security_Survey_June_2005.pdf***.

9. *See* U.S. Attorney's Office, Southern District of Florida, Press Release (July 19, 2006), available at ***http://www.usdoj.gov/usao/fls/PressReleases/060719-01.html***.

10. *See, e.g.*, John Leland, *Meth Users, Attuned to Detail, Add Another Habit: ID Theft*, New York Times, July 11, 2006, available at ***http://www.nytimes.com/2006/07/11/us/11meth.html?ex=1153540800&en=7b6c7773afa880be&ei=5070***; Byron Acohido and Jon Swartz, ***Meth addicts' other habit: Online Theft***, USA Today, December 14, 2005, available at ***http://www.usatoday.com/tech/news/internetprivacy/2005-12-14-meth-online-theft_x.htm***.

11. Bob Mims, *Id Theft Is the No. 1 Runaway U.S. Crime*, The Salt Lake Tribune, May 3, 2006, available at 2006 WLNR 7592526.

12. Dennis Tomboy, *Meth Addicts Stealing Mail*, Deseret Morning News, April 28, 2005, ***http://deseretnews.com/dn/view/0,1249,600129714,00.html.***

13. Stephen Mihm, *Dumpster-Diving for Your Identity*, New York Times Magazine, December 21, 2003, available at ***http://www.nytimes.com/2003/12/21/magazine/21IDENTITY.html?ex=1387342800&en=b693eef01223bc3b&ei=5007&partner=USERLAND.***

14. Pub. L. No. 108-159, 117 Stat. 1952.

15. The FACT Act required merchants to comply with this truncation provision within three years of the Act's passage with respect to any cash register or device that was in use before January 1, 2005, and within one year of the Act's passage with respect to any cash register or device that was first put into use on or after January 1, 2005. 15 U.S.C. § 1681c(g)(3).

16. *Overview of Attack Trends*, CERT Coordination Center 2002, available at ***http://www.cert.org/archive/pdf/attack_trends.pdf.***

17. Lanowitz, T., Gartner Research ID Number G00127407: December 1, 2005.

18. *"Vishing" Is Latest Twist In Identity Theft Scam,* Consumer Affairs, July 24, 2006, available at ***http://www.consumeraffairs.com/news04/2006/07/scam_vishing.html.***

19. Fraudsters have recently used pretexting techniques to obtain phone records, *see, e.g.*, Jonathan Krim, *Online Data Gets Personal: Cell Phone Records For Sale*, Washington Post, July 13, 2005, available at 2005 WLNR 10979279, and the FTC is pursuing enforcement actions against them. *See* ***http://www.ftc.gov/opa/2006/05/phonerecords.htm.***

20. The FTC brought three cases after sting operations against financial pretexters. Information on the settlement of those cases is available at ***http://www.ftc.gov/opa/2002/03/pretextingsettlements.htm.***

21. *See, e.g., Computers Stolen with Data on 72,000 Medicaid Recipients*, Cincinnati Enquirer, June 3, 2006.

22. 15 U.S.C. § 1681e; 15 U.S.C. § 6802(a).

23. Although the FACT Act amendments to the Fair Credit Reporting Act require merchants to truncate credit account numbers, allowing only the final five digits to appear on an electronically generated receipt, 15 U.S.C. § 1618c(g), manually created receipts might still contain the full account number.

24. *See* ***http://www.bizjournals.com/philadelphia/stories/2006/07/24/daily30.html.*** *See also* Identity Theft Resource Center, Fact Sheet 126: *Checking Account Takeover and Check Fraud,* ***http://www.idtheftcenter.org/vg126.shtml.***

25. For example, the Securities and Exchange Commission instituted proceedings against a 19-year-old internet hacker after the hacker illicitly accessed an investor's online brokerage account. His bogus transactions saved the hacker approximately $37,000 in trading losses. The SEC also obtained an emergency asset freeze to halt an Estonia-based "account intrusion" scheme that targeted online brokerage accounts in the U.S. to manipulate the markets. *See* Litigation Release No. 19949 (Dec. 19, 2006), available at ***http://www.sec.gov/litigation/litreleases/2006/lr19949.htm.***

26. For unauthorized credit card charges, the Fair Credit Billing Act limits consumer liability to a maximum of $50 per account. 15 U.S.C. § 1643. For bank account fraud, different laws determine consumers' legal remedies based on the type of fraud that occurred. For example, applicable state laws protect consumers against fraud committed by a thief using paper documents, like stolen or counterfeit checks. If, however, the thief used an electronic fund transfer, federal law applies. The Electronic Fund Transfer Act limits consumer liability for unauthorized transactions involving an ATM or debit card, depending on how quickly the consumer reports the loss or theft of his card: (1) if reported within two business days of discovery, the consumer's losses are limited to a maximum of $50; (2) if reported more than two business days after discovery, but within 60 days of the transmittal date of the account statement containing unauthorized transactions, he could lose up to $500; and (3) if reported more than 60 days after the transmittal date of the account statement containing unauthorized transactions, he could face unlimited liability. 15 U.S.C. § 1693g. As a matter of policy, some credit and debit card companies waive liability under some circumstances, freeing the consumer from fraudulent use of his credit or debit card.

27. *See* John Leland, *Some ID Theft Is Not For Profit, But to Get a Job*, N.Y. Times, Sept. 4, 2006.

28. *See* World Privacy Forum, *Medical Identity Theft: The Information Crime That Can Kill You* (May 3, 2006), available at ***worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf.***

29. *See* ***http://www.idanalytics.com/news_and_events/20051208.htm.*** Some other organizations have begun conducting statistical analyses to determine the link between data breaches and identity theft. These efforts are still in their early stages, however.

30. Government Accounting Office, *Social Security Numbers: Government Could Do More to Reduce Display in Public Records and On Identity Cards* (November 2004), at 2, available at ***http://www.gao.gov/new.items/d0559.pdf.***

31. 15 U.S.C. §§ 6801 et seq.; 42 U.S.C. §§ 1320d et seq.; 18 U.S.C. §§ 2721 et seq.

32. 5 U.S.C. § 552a.

33. *See, e.g.*, Ariz. Rev. Stat. § 44-1373.

34. *Social Security Numbers: Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain*, GAO - 05-1016T, September 15, 2005.

35. *See, e.g., www.wpsic.com/edi/comm_sub_p.shtml?mm=3, Non-SSN Member Numbers to Be Assigned for Privacy Protection.*

36. Except where expressly noted, all references to years in this strategic plan are intended to refer to calendar years, rather than fiscal years.

37. The federal government's overall information privacy program derives primarily from five statutes that assign OMB policy and oversight responsibilities, and agencies responsibility for implementation. The Privacy Act of 1974 (5 U.S.C. § 552a) sets collection, maintenance, and disclosure conditions; access and amendment rights and notice and record-keeping requirements with respect to personally identifiable information retrieved by name or personal identifier. The Computer Matching and Privacy Protection Act of 1988 (5 U.S.C. § 552a note) amended the Privacy Act to provide a framework for the electronic comparison of personnel and benefits-related information systems. The Paperwork Reduction Act of 1995 (44 U.S.C. § 3501 et seq.) and the Information Technology Management Reform Act of 1996 (also known as Clinger-Cohen Act; 41 U.S.C. § 251 note) linked agency privacy activities to information technology and information resources management, and assigned to agency Chief Information Officers (CIO) the responsibility to ensure implementation of privacy programs within their respective agencies. Finally, Section 208 of the E-Government Act of 2002 (44 U.S.C. § 3501 note) included provisions requiring agencies to conduct privacy impact assessments on new or substantially altered information technology systems and electronic information collections, and post web privacy policies at major entry points to their Internet sites. These provisions are discussed in OMB memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002."

38. *See Protection of Sensitive Agency Information*, Memorandum from Clay Johnson III, Deputy Director for Management, OMB, to Heads of Departments and Agencies, M-06-16 (June 23, 2006).

39. The United States Computer Emergency Readiness Team (US-CERT) has played an important role in public sector data security. US-CERT is a partnership between DHS and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. The organization interacts with federal agencies, state and local governments, industry professionals, and others to improve information sharing and incident response coordination and to reduce cyber threats and vulnerabilities. US-CERT provides the following support: (1) cyber security event monitoring; (2) advanced warning on emerging threats; (3) incident response capabilities for federal and state agencies; (4) malware analysis and recovery support; (5) trends and analysis reporting tools; and (6) other support services in the area of cyber security. US-CERT also provides consumer and business education on Internet and information security.

40. *See* ***http://www.whitehouse.gov/results/agenda/scorecard.html.***

41. The proposed routine use language set forth in Appendix B differs slightly from that included in the Task Force's interim recommendations in that it further clarifies, among other things, the categories of users and the circumstances under which disclosure would be "necessary and proper" in accordance with the OMB's guidance on this issue.

42. 15 U.S.C. §§ 6801-09; 16 C.F.R. Part 313 (FTC); 12 C.F.R. Part 30, App. B (OCC, national banks); 12 C.F.R. Part 208, App. D-2 and Part 225, App. F (FRB, state member banks and holding companies); 12 C.F.R. Part 364, App. B (FDIC, state non-member banks); 12 C.F.R. Part 570, App. B (OTS, savings associations); 12 C.F.R. Part 748, App. A (NCUA, credit unions); 16 C.F.R. Part 314 (FTC, financial institutions that are not regulated by the FRB, FDIC, OCC, OTS, NCUA, CFTC, or SEC); 17 C.F.R. Part 248.30 (SEC); 17 C.F.R. Part 160.30 (CFTC).

43. 15 U.S.C. § 45(a). Further, the federal bank regulatory agencies have authority to enforce Section 5 of the FTC Act against entities over which they have jurisdiction. *See* 15 U.S.C. §§ 6801-09.

44. 15 U.S.C. §§ 1681-1681x, as amended.

45. Pub. L. No. 108-159, 117 Stat. 1952.

46. 42 U.S.C. §§ 1320d et seq.

47. 31 U.S.C. § 5318(l).

48. 18 U.S.C. §§ 2721 et seq.

49. *http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.*

50. *http://www.bbb.org/securityandprivacy/SecurityPrivacyMadeSimpler.pdf; www.staysafeonline.org/basics/company/basic_tips.html; The Financial Services Roundtable, Voluntary Guidelines for Consumer Confidence in Online Financial Services*, available at *www.bitsinfo.org/downloads/Publications%20Page/bitsconscon.pdf; www.realtor.org/realtororg.nsf/files/NARInternetSecurityGuide.pdf/$FILE/NARInternetSecurityGuide.pdf; www.antiphishing.org/reports/bestpracticesforisps.pdf; www.uschamber.com/sb/security/default.htm; www.truste.org/pdf/SecurityGuidelines.pdf; www.the-dma.org/privacy/informationsecurity.shtml; http://www.staysafeonline.org/basics/company/basic_tips.html.*

51. These changes may be attributable to requirements contained in the regulations implementing Title V of the GLB Act. *See* 12 C.F.R. Part 30, App. B (national banks); 12 C.F.R. Part 208, App. D-2 and Part 225, App. 5 (state member banks and holding companies); 12 C.F.R. Part 364, App. B (state non-member banks); 12 C.F.R. Part 570, App. B (savings associations); 12 C.F.R. Part 748, App. A and B, and 12 C.F.R. Part 717 (credit unions); 16 C.F.R. Part 314 (financial institutions that are not regulated by the FDIC, FRB, NCUA, OCC, or OTS).

52. *See, e.g., http://www.truste.org/pdf/SecurityGuidelines.pdf; http://www.the-dma.org/privacy/informationsecurity.shtml.*

53. Deloitte Financial Services, *2006 Global Security Survey*, available at ***http://singe.rucus.net/blog/archives/756-Deloitte-Security-Surveys.html.***

54. Datalink, *Data Storage Security Study*, March 2006, available at ***www.datalink.com/security/.***

55. *Id.*

56. *See* Small Business Technology Institute, *Small Business Information Security Readiness* (July 2005).

57. *See, e.g.*, California (Cal. Civ. Code § 1798.82 (2006)); Illinois (815 Ill. Comp. Stat 530/5 (2005)); Louisiana (La. Rev. Stat. 51:3074 (2006)); Rhode Island (R.I. Gen. Laws § 11-49.2.3 (2006)).

58. *See, e.g.*, Colorado (Colo. Rev. Stat. § 6-1-716 (2006)); Florida (Fla. Stat. § 817.5681 (2005)); New York (NY CLS Gen. Bus. § 889-aa (2006)); Ohio (Ohio Rev. Code Ann. § 1349.19 (2006)).

59. Ponemon Institute LLC, *Benchmark Study of European and U.S. Corporate Privacy Practices*, p. 16 (Apr. 26, 2006).

60. *Id.*

61. Ponemon Institute, LLC, 2005 *Benchmark Study of Corporate Privacy Practices* (July 11, 2005).

62. MultiChannel Merchant, *Retailers Need to Provide Greater Data Security, Survey Says* (Dec. 1, 2005), available at ***http://multichannelmerchant.com/opsandfulfillment/advisor/retailers_data_security_1201/index.html.***

63. *See* Information Technology Examination Handbook's Information Security Booklet, available at ***http://www.ffiec.gov/guides.htm.***

64. *See, e.g.*, ***http://www.pvkansas.com/police/crime/iden_theft.shtml*** (Prairie Village, Kansas), ***http://phoenix.gov//POLICE/dcd1.html*** (Phoenix, Arizona); ***www.co.arapahoe.co.us/departments/SH/index.asp*** (Arapahoe County, Colorado).

65. *Colleges Are Textbook Cases of Cybersecurity Breaches*, USA TODAY, August 1, 2006.

66. Examples of this outreach include a wide-scale effort at the University of Michigan which launched Identity Web, a comprehensive site based on the recommendations of a graduate class in fall of 2003. The State University of New York's Orange County Community College offers identity theft seminars, the result of a student who fell victim to a scam. A video at student orientation sessions at Drexel University in Philadelphia warns students of the dangers of identity theft on social networking sites. Bowling Green State University in Kentucky emails campus-wide "fraud alerts" when it suspects that a scam is being targeted to its students. In recent years, more colleges and universities have hired chief privacy officers, focusing greater attention on the harms that can result from the misuse of students' information.

67. *See* 31 C.F.R. § 103.121 (banks, savings associations, credit unions, and certain non-federally regulated banks); 31 C.F.R. § 103.122 (broker-dealers); 17 C.F.R. § 270.0-11, 31 C.F.R. § 103.131 (mutual funds); and 31 C.F.R. § 103.123 (futures commission merchants and introducing brokers).

68. *See http://www.dhs.gov/xprevprot/laws/gc_1172765386179.shtm.*

69. A primary reason criminals use other people's identities to commit identity theft is to enable them to operate with anonymity. However, in committing identity theft, the suspects often leave telltale signs that should trigger concern for alert businesses. Section 114 of the FACT Act seeks to take advantage of businesses' awareness of these patterns, and requires the federal bank regulatory agencies and the FTC to develop regulations and guidelines for financial institutions and creditors addressing identity theft. In developing the guidelines, the agencies must identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft. 15 U.S.C. § 1681m.

    Those agencies have issued a set of proposed regulations that would require each financial institution and creditor to develop and implement an identity theft prevention program that includes policies and procedures for detecting, preventing, and mitigating identity theft in connection with account openings and existing accounts. The proposed regulations include guidelines listing patterns, practices, and specific forms of activity that should raise a "red flag" signaling a possible risk of identity theft. Recognizing these "red flags" can enable businesses to detect identity theft at its early stages before too much harm is done. *See* 71 Fed. Reg. 40786 (July 18, 2006) to be codified at 12 C.F.R. Parts 41 (OCC), 222 (FRB), 334 and 364 (FDIC), 571 (OTS), 717 (NCUA), and 16 C.F.R. Part 681 (FTC), available at *http://www.occ.gov/fr/fedregister/71fr40786.pdf.*

70. USB token devices are typically small vehicles for storing data. They are difficult to duplicate and are tamper-resistant. The USB token is plugged directly into the USB port of a computer, avoiding the need for any special hardware on the user's computer. However, a login and password are still required to access the information contained on the device. Smart cards resemble a credit card and contain a microprocessor that allows them to store and retain information. Smart cards are inserted into a compatible reader and, if recognized, may require a password to perform a transaction. Finally, the common token system involves a device that generates a one-time password at predetermined intervals. Typically, this password would be used in conjunction with other login information such as a PIN to allow access to a computer network. This system is frequently used to allow for remote access to a work station for a telecommuter.

71. Biometrics are automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. Biometrics commonly implemented or studied include: fingerprint, face, iris, voice, signature, and hand geometry. Many other modalities are in various stages of development and assessment. Additional information on biometric technologies, federal biometric programs, and associated privacy considerations can be found at *www.biometrics.gov*.

72. *See Authentication in an Internet Banking Environment* (October 12, 2005), available at ***http://www.ffiec.gov/pdf/authentication_guidance.pdf***.

73. *See* FFIEC Frequently Asked Questions on *FFIEC Guidance on Authentication in an Internet Banking Environment* (August 15, 2006), available at ***http://www.ffiec.gov/pdf/authentication_faq.pdf***.

74. *See* Kristin Davis and Jessica Anderson, *But Officer, That Isn't Me*, Kiplinger's Personal Finance (October 2005); Bob Sullivan, *The Darkest Side of ID Theft*, MSNBC.com (Dec. 1, 2003); David Brietkopf, *State of Va. Creates Special Cards for Crime Victims*, The American Banker (Nov. 18, 2003).

75. 18 U.S.C. § 1028A.

76. 18 U.S.C. § 1028(d)(7).

77. *See* 18 U.S.C. § 1030(e)(8).

78. 18 U.S.C. § 1030(a)(7).

79. S. Rep. No. 105-274, at 9 (1998).

80. As this Task Force has been charged with considering the federal response to identity theft, this routine use notice does not include all possible triggers, such as embarrassment or harm to reputation. However, after consideration of the Strategic Plan and the work of other groups charged with assessing Privacy Act considerations, OMB may determine that a routine use that takes into account other possible triggers may be preferable.

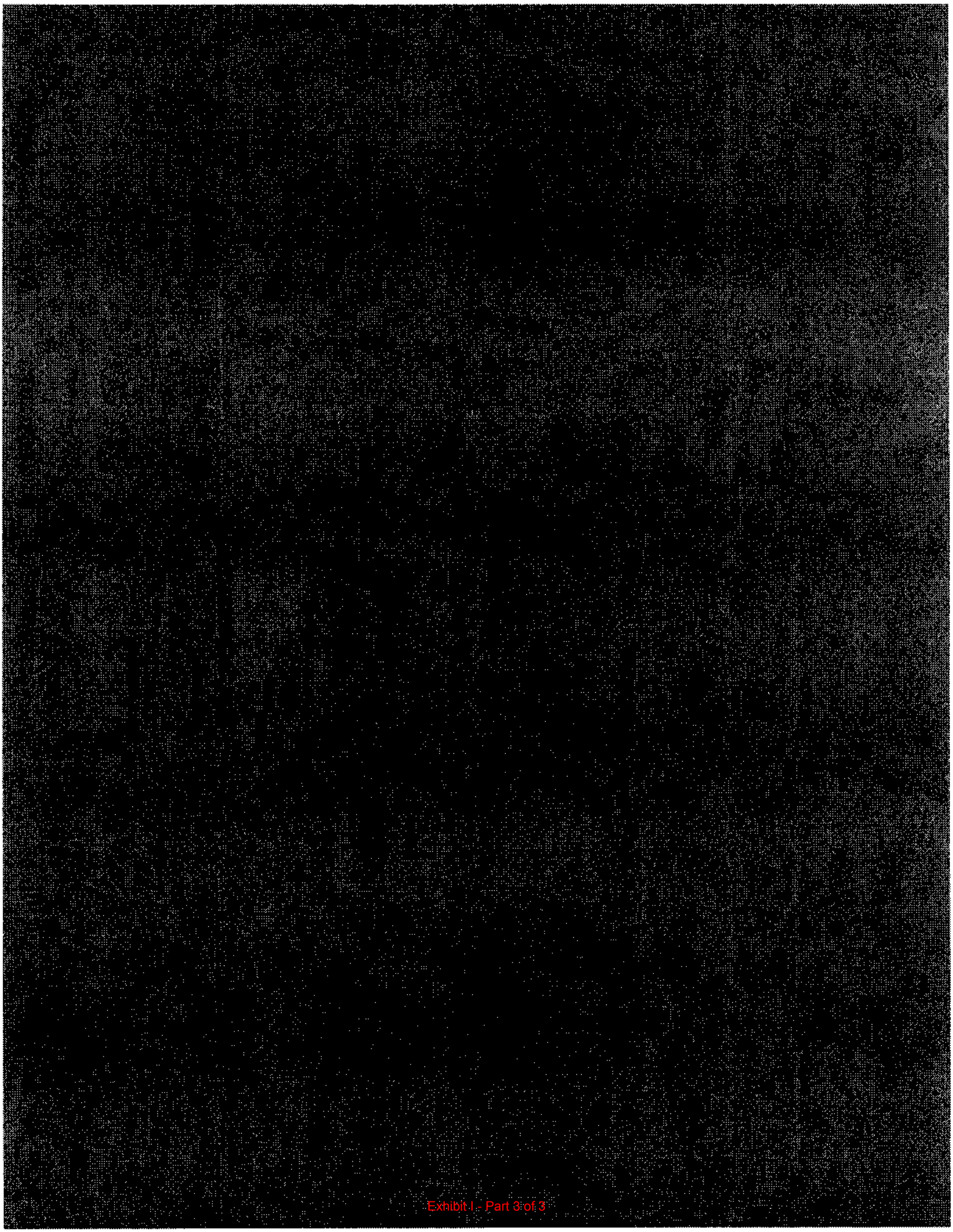

Exhibit I - Part 3 of 3