

SUBMISSION TO THE PRESIDENT'S IDENTITY THEFT TASK FORCE

Friday, January 19, 2007

The Honorable Alberto R. Gonzales
Attorney General
United States of America
Department of Justice
Washington, D.C. 20530

The Honorable Deborah Platt Majoras
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Attorney General Gonzales and Chairman Majoras:

The Business Software Alliance (BSA)¹ continues to offer its strong support for the *President's Identity Theft Task Force*. BSA is confident that the Task Force will make a critical contribution to maintaining consumer confidence in the Internet and e-commerce. Through this submission, BSA would like to emphasize some of the suggestions it had made in its letter of December 22, 2006.

I. Maintaining security of consumer data

National data security standards

The Congress is considering imposing national data security requirements on all entities that maintain sensitive consumer information. If such requirements were to be enacted, BSA believes that they should be effective, flexible and technologically neutral.

These measures should rely on a risk-based approach that requires organizations to assess their operations and IT systems and decide what measures are safe, appropriate and cost-effective. To this end, when Government agencies are enforcing and interpreting a prospective data breach notification statute, they should permit various approaches and solutions to protect data in electronic form. Therefore, it is crucial to their effectiveness

¹ **About the BSA:** The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, CA, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Dell, Entrust, HP, IBM, Intel, McAfee, Microsoft, Monotype Imaging, PTC, EMC, SAP, SolidWorks, Sybase, Symantec, Synopsys, The MathWorks, and UGS.

that national data security standards not require the deployment or use of specific products or technologies, including any specific computer hardware or software.

Proper allocation of liability

The companies or individuals who own or license electronic data are responsible for protecting that data. A company that designs, develops or sells security products should not be penalized because the entity which suffered a data breach did not take adequate security measures. Therefore, a person developing or providing computer hardware or software should not be found to be in violation of information security rules because a person using that product is found to be in violation of those rules.

Breach notice requirements

BSA believes that a breach notification requirement yields two important benefits. First, if properly designed, breach notification provides consumers with needed information to enable them to protect themselves. Second, breach notification also encourages organizations that hold consumer data to implement increased data security measures.

Hereafter, BSA proposes some of the essential elements of an effective breach notification requirement:

- Prevent over notification

Currently, notification of a data breach is required by 33 states. Many require notification in all instances. As a result, consumers and businesses are likely to become immune to reports of data breaches and fail to take appropriate action.

A more effective notification provision would include language that would require notification only in those instances where an unauthorized disclosure presents a significant risk of material harm from identity theft.

- Exclude data that has been rendered unusable, unreadable or indecipherable

BSA believes data security can be enhanced without a significant and difficult to enforce regulatory system by providing a market-based incentive. This can be done through an exception, to the proposed obligation to notify security breaches, in cases where the data is protected so that even if it "gets out" the information cannot be used.

To qualify for this exception, a security measure must provide genuine, effective consumer protection. BSA believes this can be achieved if the measure in question satisfies two conditions. First, it must render data "unusable, unreadable or indecipherable" to any party that gains unauthorized access. Second, it must also be "widely accepted as an effective industry practice or an industry standard". Examples of such measures include encryption, redaction, and access controls. Under these two conditions, the data that has been accessed cannot be used to defraud or inflict harm on data subjects. Therefore, the apparent breach is not a real breach and does not need to be notified.

BSA also believes that any proposed changes to the law should introduce a rebuttable presumption. If the data has been protected with a measure that qualifies for the exception, the presumption would be that no significant risk of harm exists; therefore, the

breach would not need to be notified. However, this presumption would be rebutted if an analysis of the circumstances of the breach shows the measure in question has been compromised or is reasonably likely to be compromised.

- Appropriate enforcement

BSA supports granting federal and state Attorneys General powers of enforcement of a federal data breach law. However, BSA believes it is important to prevent excessive litigation. Allowing private lawsuits merely as a result of the occurrence of a data breach would yield little security benefits to consumers. It would also create the risk that some data custodians refrain from notifying consumers in case of breaches, for fear of opening themselves to lawsuits.

Therefore, federal legislation must explicitly state that breach notification law is not the basis for an individual or class action lawsuit.

- Establish a national standard

Currently, a plethora of state data breach laws have been enacted and several more States still have bills pending. This patchwork of state laws has created widespread confusion and difficulties: for businesses which have to comply with a multitude of standards, and for consumers who receive notices from a variety of sources.

Federal legislation establishing one national framework would benefit businesses and consumers alike. It would need to clarify that it preempts state data security and data breach laws.

Education of the private sector and consumers on safeguarding data

BSA believes that increasing education and awareness is an important component of any effort to decrease the incidence of identity theft. BSA strongly recommends that the Administration maintain its support of private-public partnerships, like the National Cyber Security Alliance (NCSA). The NCSA is a 501(c)3 non-profit organization designed to educate consumers, businesses, K-12 and higher education audiences on how they can stay safe online and protect their information. The NCSA just completed a 2006 TV and Radio Public Service Announcement on identify theft and how consumers and businesses can protect their information. The NCSA already has a number of initiatives underway for 2007.

BSA believes that, by combining federal and corporate resources, the public and private sectors can work together to solve these important issues and better educate all audiences and stakeholders.

II. Law enforcement: prosecuting and punishing identity thieves

Establishing a National Identity Theft Law Enforcement Center

BSA believes that a robust marketplace of ideas is the ideal way to combat cyber criminals and identity thieves. But overcoming these challenges will require not only innovative technologies, but also innovative partnerships between industry and government. BSA

works with the National Cyber Forensics and Training Alliance² (NCFTA), a non-profit consortium which provides a neutral collaborative venue where critical confidential information about cyber incidents can be shared voluntarily and discreetly among industry, academia and law enforcement. The NCFTA also facilitates advanced training, promotes security awareness to reduce cyber-vulnerability, and conducts forensic and predictive analysis and lab simulations. These activities are intended to educate organizations and enhance their abilities to manage risk and develop security strategies and best practices.

The NCFTA is the first partnership of its kind in the nation. Future partnerships will be established in regions where interest exists to combine resources, intelligence, and expertise more effectively. These additional partnerships will be linked together, enhancing the resources fundamental to their mission. This coordinated and decentralized approach will empower regional teams with vital information and expertise in a timely and efficient manner. BSA encourages the Task Force to reach out to the NCFTA to discuss how best to establish an identity theft information sharing model.

Investigation and prosecution of identity thieves who reside in foreign countries

The global nature of the Internet allows cyber criminals to carry out identity theft, online fraud and other illicit schemes from nearly anywhere in the world, leaving billions of dollars in damage and the slim chance of punishment for their crimes. As a result, identity theft and cybercrime inherently becomes an international issue that requires international solutions. BSA has long been a strong advocate of the Council of Europe Convention on Cybercrime and applauded the U.S. Government's recent ratification of the Convention. The Convention on Cybercrime is a vital step toward establishing the international cooperation and deterrence necessary to tackle this very global problem. To truly maximize the effectiveness of the Convention, the U.S. Government must urge the remaining signatory countries that have not ratified to follow the U.S.'s lead and complete the ratification process. The U.S. Government can also reach out to other countries, particularly Russia and countries in Asia to enact suitable cybercrime laws and adopt the Cybercrime Convention.

Amendments to federal statutes and guidelines used to prosecute identity-theft related offenses

BSA continues to recognize the critical importance of maintaining confidence in the Internet and e-commerce. Unfortunately, online confidence is being threatened by increasingly sophisticated and organized criminal elements who threaten to steal identities, defraud users, and commit extortion online. Identity thieves and cyber criminals are taking advantage of blind spots in current criminal statutes relating to cyber crime. BSA strongly supports legislation that fills gaps in the criminal code and gives law enforcement the tools necessary to effectively find and prosecute cyber criminals.

The following are measures that we strongly advocate:

- Criminalizing malicious botnet attacks

² National Cyber Forensics and Training Alliance (NCFTA) : <http://www.ncfta.net>

Increasingly, individuals who perpetuate harm through the use of computers do so by accessing and controlling protected computers remotely and without authorization. The compromised computers thus become “botnets” – a “robot network” of compromised “zombie” computers remotely controlled by an attacker. Botnets represent a significant danger because the people who control botnets, often referred to as “Bot Herders,” can build botnets that involve several hundred thousand machines. These machines can be used to attack other machines, perpetrate identity theft, spread spyware, or disrupt Internet functions.

Generally, current law is not well-tailored to support prosecution of Bot Herders. Even when a botnet is large, it may be difficult for prosecutors to prove the damage necessary for a prosecution under current 18 USC Sec. 1030(a)(5). In addition, prosecutors may be reluctant to charge the creator of a botnet under the current section 1030(a)(2), because it may be difficult to prove that the Bot Herder “obtained information” from one of the attacked zombie computers. Identifying, stopping, and prosecuting Bot Herders is critical for all users, including both consumers and critical infrastructures. Discovering and shutting down a Botnet is tantamount to identifying the precursors to and preventing identity theft, network disruption, and loss of intellectual property. Botnets can result in widespread damage and deserve immediate attention. Cyber criminals are commoditizing botnets and selling them to other would-be attackers. Trafficking of these attack tools can fund any number of other illegal activities. Additionally, the methodologies for assembling, and controlling botnets are becoming increasingly sophisticated and difficult to trace.

To greatly aid prosecutions of Bot Herders, 18 USC Sec. 1030(a)(2) can be modified to explicitly cover means of identification of bot herders. 18 USC Sec. 1030(a)(5) also can be modified to criminalize causing damage to 10 or more protected computers in any one-year period, without having to necessarily prove at least \$5000 damage to any one protected computer. This change would allow prosecution of those who covertly install malicious bots on protected computers for the purposes of making a malicious botnet, even if the \$5000 damage threshold can not be proven.

- Eliminating interstate communications requirement for cybercrime

Today US code related to cybercrime, 18 USC Sec.1030, only guards against unauthorized access to a computer which is used in interstate or foreign commerce or communications and necessitates that the cyber criminal’s conduct in obtaining information from such a computer itself involved an interstate or foreign communication. Broadening the coverage of this statute by eliminating the requirement in current law that criminal conduct itself involve an interstate or foreign communication will effectively close loopholes that currently inhibit legitimate cases. The statute should be strengthened to provide that a protected computer also is one which *affects* interstate commerce and that it is illegal to obtain information from any protected computer without authorization.

- Covering cyber racketeering through the addition of RICO predicates

RICO predicate offenses should be updated to give U.S. law enforcement the legal ability to effectively investigate and prosecute organized crime syndicates. Organized crime syndicates from Eastern Europe, Africa, Asia and other regions have been identified as

significant culprits behind phishing scams, identity theft, online extortion and other cybercrime activities. Action should be taken to update the predicate offenses to support a racketeering criminal charge.

- Covering cyber extortion

Existing definitions of extortion in 18 U.S.C. §§ 875 and 1030 criminalize threats communicated with the intent to extort "money or other thing of value." Some threats, which may be terrifying and damaging, do not demand "things," but instead demand that the recipient refrain from lawful conduct or suffer denial of service attacks, posting of confidential information online, and identity theft. The threats do not demand either money or things of value. While cyber criminals often threaten online businesses with cyber-attacks for the purposes of extorting money, cyber extorters often harass and attack without explicit demands for things of value. Rather some extorters may seek to cripple a competitor's online services or carry through on a vendetta. Spamhaus.org is an international non-profit organization whose stated mission is "to track the Internet's Spam Gangs, to work with Law Enforcement Agencies to identify and pursue spammers worldwide." They and a number of high profile anti-spam organizations have been the frequent target of denial-of-service attacks (the most common cyber extortion tool) from the combined efforts of spammers, hackers, and virus writers. The spammers did not attack to extort money, but rather wished to cripple organizations and services that had blacklisted them. Updating criminal statutes to address this type of cyber extortion is vital to the protection of law-abiding citizens.

- Including conspiracy to commit cybercrime

As organized crime becomes more involved in cybercrime, focusing the penalty structure on illegal group behavior becomes more important. Adding an explicit conspiracy charge to § 1030, rather than relying upon the general criminal conspiracy statute in 18 U.S.C. § 371, would not only subject conspiracy recidivists to enhanced penalties under § 1030 but also treat conspiracies to commit such offenses similarly to attempts, which are arguably less egregious than illegal group activity and are explicitly criminalized in this statute.

- Forfeiting property used to commit cybercrime

Property, both real and personal, that is derived from proceeds traceable to a violation of 18 U.S.C. § 1030 is currently subject to both criminal and civil forfeiture. We believe that forfeiture should include computers, equipment, and other personal property used to violate the CFAA, as well as real and personal property derived from the proceeds of computer crime.

- Expanding sentencing guidelines

Currently, sentences for violations of 18 U.S.C. § 1030 are determined by calculating actual economic loss, which is often difficult to determine in the computer crime context. Defendants convicted of computer crimes often serve no term of imprisonment, resulting in the absence of any deterrent effect arising from criminal prosecution and making

computer crimes less likely to be prosecuted in the future. The U.S. Sentencing Commission should be directed, in determining its guidance on the appropriate sentence for computer crime, to consider a number of highly relevant factors in order to create an effective deterrent to computer crime.

- Increasing funding for law enforcement to fight cybercrime

The need for more dedicated law enforcement personnel and advanced forensic tools to investigate and assist in the prosecution of computer crimes is greater than ever. Identity thieves and other cyber criminals continuously evolve their schemes and frauds to deceive users, outmaneuver authorities, and even compete with each other. It is essential that law enforcement has the resources necessary to hire and train additional law enforcement officers dedicated to investigating crimes committed through the use of computers and other information technology, including through use of the Internet, and for the procurement of advanced tools of forensic science to investigate and study such crimes.

Thank you for considering our views on the important issue of identity theft. The BSA looks forward to continuing to work with the Department of Justice and Federal Trade Commission.

Sincerely yours,

Robert W. Holleyman, II
President & CEO
Business Software Alliance



DPM, BCP, Idusman
Kaufman 9715816

Robert W. Holleyman, II
President and Chief Executive Officer

1150 18th Street, NW
Suite 700
Washington, DC 20036

p. 202/872.5500
f. 202/872.5501

December 22, 2006

The Honorable Alberto R. Gonzales
Attorney General
United States of America
Department of Justice
Washington, D.C. 20530

The Honorable Deborah Platt Majoras
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Attorney General Gonzales and Chairman Majoras:

The Business Software Alliance (BSA)* continues to offer its strong support for the *President's Identity Theft Task Force* created earlier this year. BSA is confident that the Task Force will make a critical contribution to maintaining consumer confidence in the Internet and e-commerce. Through this letter, BSA submits several suggestions on potential policy initiatives that the Task Force may recommend.

Effective, risk-based data breach legislation

BSA has been deeply involved in the debate over federal data breach legislation. BSA believes that legislation in this area should seek to achieve the following goals:

1. Preclude specific government technology mandates

Safeguards against data breaches should be effective, flexible and technologically neutral for organizations that handle consumer data. These measures should rely on a risk-based approach that requires organizations to assess their operations and IT systems and decide what measures are safe, appropriate and cost-effective. Thus, when Government agencies are enforcing and interpreting a prospective data breach notification statute, they should permit various approaches and solutions to protect data in electronic form and not require the deployment or use of specific products or technologies, including any specific computer hardware or software.

2. Establish liability protection

The companies or individuals who own or license electronic data are responsible for protecting that data. A company that designs, develops or sells security products should not be penalized because the entity which suffered a data breach did not take adequate



security measures. A person developing or providing computer hardware or software should not be found to be in violation of information security rules because a person using that product is found to be in violation of those rules.

3. Prevent over notification

Currently, notification of a data breach is required by 33 states and many require notification in all instances. As a result, consumers and businesses are likely to become immune to reports of data breaches and fail to take appropriate action. A more effective notification provision would include language that would require notification only in those instances where an unauthorized disclosure presents a significant risk of material harm from identity theft.

4. Exclude data that has been rendered unusable, unreadable or indecipherable

BSA believes that greater security is more readily achieved with positive incentives rather than through sanctions. One way to enhance data security without a significant and difficult to enforce regulatory system is to provide a safe harbor from the proposed obligation to notify security breaches in those cases where the data is protected so that even if it "gets out" the information cannot be used.

To qualify for the safe harbor, a security measure must provide genuine, effective consumer protection. BSA believes this can be achieved if the measure in question satisfies two conditions. First, it must render data "unusable, unreadable or indecipherable" to any party that gains unauthorized access. Second, it must also be "widely accepted as an effective industry practice or an industry standard". Under these two conditions, the data that has been accessed cannot be used to defraud or inflict harm on data subjects. Therefore, the apparent breach is not a real breach and does not need to be notified.

BSA also believes that the any proposed changes to the law should introduce a rebuttable presumption. If the data has been protected with a measure that qualifies for the safe harbor, the presumption would be that no significant risk of harm exists; therefore, the breach would not need to be notified. However, this presumption would be rebutted if an analysis of the circumstances of the breach shows the measure in question has been compromised or is reasonably likely to be compromised.

BSA believes that such a safe harbor would be a powerful incentive to implement effective data security practices or methods that may not otherwise be implemented. This is because a safe harbor gives data controllers and processors a reasonable assurance that, if they use security measures that render the data unusable, unreadable or indecipherable, they will avoid liability or reputation damage.

5. Appropriate enforcement

BSA supports granting federal and state Attorney Generals powers of enforcement of a federal data breach law. However, BSA believes it is important to curb prevent excessive litigation. Allowing private lawsuits merely as a result of the occurrence of a data breach would yield little security benefits to consumers. It would also create the risk that some data custodians refrain from notifying consumers in case of breaches, for fear of opening themselves to lawsuits.

Therefore, federal legislation must explicitly state that breach notification law is not the basis for an individual or class action lawsuit.

6. Establish a national standard

Currently, a plethora of state data breach laws have been enacted and several more States still have bills pending. This patchwork of State laws has created widespread confusion and difficulties for businesses which have to comply with a multitude of standards, and for consumers who receive notices from a variety of sources. Federal legislation establishing one national framework would benefit businesses and consumers alike. It would need to clarify that it preempts state data security and data breach laws.

Giving U.S. law enforcement officials the tools necessary to find and prosecute cyber criminals

BSA continues to recognize the critical importance of maintaining confidence in the Internet and e-commerce. Unfortunately, online confidence is being threatened by increasingly sophisticated and organized criminal elements who are taking advantage of blind spots in current criminal statutes relating to cyber crime. BSA strongly supports legislation that fills gaps in the criminal code and gives law enforcement the tools necessary to effectively find and prosecute cyber criminals:

1. Criminalizing malicious botnet attacks

Increasingly, individuals who perpetuate harm through the use of computers do so by accessing and controlling protected computers remotely and without authorization. The compromised computers

thus become "botnets" – a "robot network" of compromised "zombie" computers remotely controlled by an attacker. Botnets represent a significant danger because the people who control botnets, often referred to as "Bot Herders," can build botnets that involve several hundred thousand machines. These machines can be used to attack other machines, spread spyware, or disrupt Internet functions.

BSA applauds the priority that the Department of Justice has given to cases involving Bot Herders, as reflected prosecutions earlier this year of criminals in California and Washington. For example, the botnet attack last year that caused the system at Seattle's Northwest Hospital to malfunction caused significant disruptions that affected the hospital's crucial systems in numerous way including: doors to the operating rooms did not open, pagers did not work and computers in the intensive care unit shut down. These are extremely serious cases and we are pleased that the Justice Department recognizes the significant threats posed to the public by botnet attacks.

While BSA is grateful for the enforcement efforts by the Justice Department, we believe that current law to support prosecutions of Bot Herders prior to an attack can be strengthened. Generally, current law is not well-tailored to support prosecution of Bot Herders. Even when a botnet is large, it may be difficult for prosecutors to prove the damage necessary for a prosecution under current 18 USC Sec. 1030 (a) (5). In addition, prosecutors may be reluctant to charge the creator of a botnet under the current section 1030(a)(2), because it may be difficult to prove that the Bot Herder "obtained information" from one of the attacked zombie computers. Identifying, stopping, and prosecuting Bot Herders is critical for all users, including both consumers and critical infrastructures. Discovering and shutting down a Botnet is tantamount to identifying the precursors to and preventing identity theft, network disruption, and loss of intellectual property. Botnets can result in widespread damage and deserve immediate attention. Cyber criminals are commoditizing botnets and selling them to other would-be attackers. Trafficking of these attack tools can fund any number of other illegal activities. Additionally, the methodologies for assembling, and controlling botnets are becoming increasingly sophisticated and difficult to trace.

To greatly aid prosecutions of bot-herders, 18 USC Sec. 1030(a)(5) can be modified to criminalize causing damage to 10 or more protected computers in any one-year period, without having to necessarily

prove at least \$5000 damage to any one protected computer. This change would allow prosecution of those who covertly install malicious bots on protected computers for the purposes of making a malicious botnet, even if the \$5000 damage threshold can not be proven.

2. **Closing loopholes in law enforcement's ability to prosecute unlawful activity**

Today US code related to cyber crime, 18 USC Sec.1030 only guards against unauthorized access to a computer which is used in interstate or foreign commerce or communications and necessitates that the cyber criminal's conduct in obtaining information from such a computer itself involved an interstate or foreign communication. Broadening the coverage of this statute by eliminating the requirement in current law that criminal conduct itself involve an interstate or foreign communication will effectively close loopholes that currently inhibit legitimate cases. The statute should be strengthened to provide that a protected computer also is one which *affects* interstate commerce and that it is illegal to obtain information from any protected computer without authorization.

3. **Covering cyber racketeering through the addition of RICO predicates**

RICO predicate offenses should be updated to give U.S. law enforcement the legal ability to effectively investigate and prosecute organized crime syndicates. Organized crime syndicates from Eastern Europe, Africa, Asia and other regions have been identified as significant culprits behind phishing scams, identity theft, online extortion and other cyber crime activities. Action should be taken to update the predicate offenses to support a racketeering criminal charge.

4. **Covering cyber extortion**

Existing definitions of extortion in 18 U.S.C. §§ 875 and 1030 criminalize threats communicated with the intent to extort "money or other thing of value." Some threats, which may be terrifying and damaging, do not demand "things," but instead demand that the recipient refrain from lawful conduct or suffer denial of service attacks, posting of confidential information online, and identity theft. The threats do not demand either money or things of value. While cyber criminals often threaten online businesses with cyber-attacks for the purposes of extorting money, cyber extorters often harass and attack without explicit demands for things of value. Rather some extorters may seek to cripple a competitor's online services or carry through on a vendetta. Spamhaus.org an

international non-profit organization whose stated mission is "to track the Internet's Spam Gangs, to work with Law Enforcement Agencies to identify and pursue spammers worldwide." They and a number of high profile anti-spam organizations have been the frequent target of denial-of-service attacks (the most common cyber extortion tool) from the combined efforts of spammers, hackers, and virus writers. The spammers did not attack to extort money, but rather wished to cripple organizations and services that had blacklisted them. Updating criminal statutes to address this type of cyber extortion is vital to the protection of law-abiding citizens.

5. Including conspiracy to commit cyber crime

As organized crime becomes more involved in cyber crime, focusing the penalty structure on illegal group behavior becomes more important. Adding an explicit conspiracy charge to § 1030, rather than relying upon the general criminal conspiracy statute in 18 U.S.C. § 371, would not only subject conspiracy recidivists to enhanced penalties under § 1030 but also treat conspiracies to commit such offenses similarly to attempts, which are arguably less egregious than illegal group activity and are explicitly criminalized in this statute.

6. Forfeiting property used to commit cyber crime

Property, both real and personal, that is derived from proceeds traceable to a violation of 18 U.S.C. § 1030 is currently subject to both criminal and civil forfeiture. We believe that forfeiture should include computers, equipment, and other personal property used to violate the CFAA, as well as real and personal property derived from the proceeds of computer crime.

7. Expanding sentencing guidelines

Currently, sentences for violations of 18 U.S.C. § 1030 are determined by calculating actual economic loss, which is often difficult to determine in the computer crime context. Defendants convicted of computer crimes often serve no term of imprisonment, resulting in the absence of any deterrent effect arising from criminal prosecution and making computer crimes less likely to be prosecuted in the future. The US Sentencing Commission should be directed, in determining its guidance on the appropriate sentence for computer crime, to consider a number of highly relevant factors in order to create an effective deterrent to computer crime.

8. Increasing funding for law enforcement to fight cyber crime

The need for more dedicated law enforcement personnel and advanced forensic tools to investigate and assist in the prosecution of

computer crimes is greater than ever. It is essential that law enforcement has the resources necessary to hire and train additional law enforcement officers dedicated to investigating crimes committed through the use of computers and other information technology, including through use of the Internet, and for the procurement of advanced tools of forensic science to investigate and study such crimes.

We thank you for considering our views on the important issue of identity theft. We look forward to continuing to work with the Department of Justice and Federal Trade Commission.

Sincerely,



Robert W. Holleyman, II
President and CEO

**The Business Software Alliance (www.bsa.org) is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace. Its members represent one of the fastest growing industries in the world. BSA programs foster technology innovation through education and policy initiatives that promote copyright protection, cyber security, trade and e-commerce. BSA members include Adobe, Apple, Autodesk, Avid, Bentley Systems, Borland, Cadence Design Systems, Cisco Systems, CNC Software/Mastercam, Dell, Entrust, HP, IBM, Intel, McAfee, Microsoft, PTC, RSA; The Security Division of EMC, SAP, SolidWorks, Sybase, Symantec, Synopsis, The MathWorks, and UGS.*