Identity Theft Resource Center
P.O. Box 26833
San Diego, CA 92196
858.693.7935
www.idtheftcenter.org

U.S. Sentencing Commission

Public Hearing on Hacking and Penalties

March 18, 2009

Written Testimony of the Identity Theft Resource Center (ITRC):

Linda Foley, Founder

Jay Foley, Executive Director

Sheila Gordon, Director of Victim Services

Rex Davis, Director of Operations

Hacking and Sentencing Penalties

Members of the committee: Thank you for the opportunity to provide both written and oral testimony for your committee today and for your interest in the topic of identity theft.

The oral portion of our testimony will be provided by Nicole Robinson, a victim of identity theft and the ITRC's North Atlantic Coast Regional Coordinator and volunteer.

The Identity Theft Resource Center (ITRC) is passionate about combating identity theft, empowering victims and consumers, assisting law enforcement, reducing business loss due to this crime and helping victims. It is critically important that in today's economic environment, companies must be assisted in the battle against electronic breaches to stay strong.

ITRC was asked to consider two scenarios in terms of sentencing:

A. A hacker steals personal information from a computer just because they can, but has no intent on using it. No person has had their identity used. No one suffers a loss.

B. A hacker steals personal information from a computer with the intent of selling or using it to steal identities. Businesses suffer a loss; ID theft victims suffer a loss.

The sentencing commission suggested that the perpetrator in scenario A would receive a shorter sentence than the perpetrator in scenario B since there were no real "victims". Under sentencing guidelines you attain victim status only when you suffer a loss.

ITRC disagrees with this presumption.

ITRC's POSITION: The sentencing guidelines in these two scenarios should be the same.

In both scenarios the company has been harmed and is a victim of the hacking. The idea that no one suffers a loss is incorrect. After studying breaches for more than four years, and working with companies that have been victimized by a hacker, ITRC can firmly say that any entity that has been hacked has been harmed. Its reputation is tainted and there is an impact on customer loyalty and trust. People get nervous and companies try to mollify them by buying expensive consumer products that affect profit/loss bottom lines. All we have to do is look at the Heartland Payment Systems breach or TJX to see how much money was spent by both the company breached as well as those financial institutions that had to replace credit cards at great expense.

According to the recently released Gartner study[1], data breaches were the leading cause of financial crimes against consumers in 2008. They also found that consumers changed behaviors based on security concerns. These are a couple of the key findings:

- *When compared to the average consumer, nearly twice as many people who lost money to fraud in 2008 changed their shopping, payments, and e-commerce behavior. Fraud victims are also more cautious about which brick-and-mortar stores they shop at and how they pay for goods when they get there, demonstrating more awareness of the risk of data breaches.*

[1] 2008 Data Breaches and Financial Crimes Scare Consumers Away, 27 February 2009, ID Number G00165825 ©Gardner Inc

- *Victims of electronic checking and/or savings account transfer fraud in 2008 were nearly five times more likely to change banks because of security concerns, when compared with the average consumer. About twice as many of the victims curtailed online money transfers and bill payment used in online banking.*

The 2007 Study of U.S. Cost of a Data Breach by the Ponemon Institute states:
The cost of lost business continued to increase at more than 30 percent, averaging $4.1 million or $128 per record compromised. Lost business now accounts for 65 percent of data breach costs compared to 54 percent in the 2006 study.

Why is intent a deciding factor? In legislative discussions in California, about information trafficking and hacking, the concept of "risk of harm" was raised. In fact, it is part of some of the security breach laws in various states and in some of the federal bills currently under consideration. With today's technology and the sophistication of crime groups which are hacking into computer systems, even PCI-compliant companies, how do we determine harm? Even if they don't use the data immediately, how do we know the information was not sold or warehoused? Is extortion considered "no intent" to use the information?

Linda Foley, Founder of the ITRC, states it this way:
First, the hacking or theft of electronic information is a malicious and harmful act. In Section 1030 of US Title 18 it states: "whoever intentionally accesses a computer without authorization or exceeds authorized access…shall be punished as provided in subsection (c) of this section." The law refers to the illegal access of a computer. There must always be considered a presumed intent to cause harm. The law already allows additional penalties for intent to defraud, extorts, cause damage to a computer, etc.

Second, there is always a victim, whether that victim is a person whose information was stolen or a company that now bears the cost and burden of trying to regain customer trust. In every hacking case there is a loss and there is a victim so the first scenario is incorrect in its assumption of "no harm."

U.S. Attorneys do not get simple cases. If a case has reached the point where U.S. Sentencing Standards apply, then the FBI or Secret Service has been involved. There are most likely other charges that can be added besides hacking if additional penalties are appropriate.

A stolen car is a stolen car. Hacking by its very nature is intrusive. When someone steals a car, does it matter if the thief purposely targets one person's car, steals a nice car to joy-ride or simply takes a car to prove they can do it? The victim is still a victim no matter for what reason the car was stolen. If additional penalties are needed because of the situation, such as vehicular damage or endangering the lives of others, then they are added.

Jay Foley, ITRC Executive Director sums it up: The key is the possession of the data. *In the scenarios provided, the hacker actually took possession of the information. Whether he intended to use it or not, he still stole the information. Therefore, the sentence should be the same as for the individual who stole it and used it. If he had just wanted to prove that he had the skills to access the information, i.e. hack the system, then he would and could only be charged for hacking and not data theft.*

The bottom line is that in the scenarios discussed above, ITRC firmly believes that businesses must receive added protection from hackers who, with or without intent to harm, breach the data systems. It is difficult to prove harm and it should be the job of the defense attorney to prove there was no intent to harm and not the prosecutor's job. Hackers, even those who are just playing around, impact the business community's ability to flourish and grow. Mandatory breach notification laws, which are found in 44 states, require that companies report electronic breaches. The need to report a breach always affects a government agency's or company's status in the eyes of consumers.

We are honored by your invitation and will continue to make our opinions available upon request to your representatives over the next few months as you grapple with this complex crime and sentencing recommendations.

In Conclusion: The Identity Theft Resource Center was invited by your commission to provide subject-matter expert testimony. It is our professional opinion that the crime is the unauthorized access of a computer database which contains personal identifying information, whether that is by a thief or an uninvited individual looking for security leaks. In both cases, the business is a victim and is harmed due to the inevitable costs of having to deal with the various consequences listed above. Breach notification laws are vital and are not to blame for this problem. The individual(s) who accessed the databases are. Both situations should have the same baseline sentence. Additional counts or penalties can be added, such as those found in U.S. Title 18, section 1030.

ABOUT ITRC:
The Identity Theft Resource Center's (ITRC) mission is to research, analyze and distribute information about the growing crime of identity theft. It serves as a resource and advisory center for consumers, victims, law enforcement, legislators, businesses, media and governmental agencies. In late 1999, Linda Foley founded this San Diego-based nonprofit program after becoming a victim of identity theft. The comments above represent the opinions of the entire management staff listed in the title.