

# ZRA™ RISK ASSESSMENT

FOR IMMEDIATE RELEASE

March 26, 2009

## CONTACT

Melissa Grondin | [mgrondin@zra.com](mailto:mgrondin@zra.com) | 703.224.8142

## Higher Penalties Reflect New Federal Approach to ID Theft, Cyber Crime

ARLINGTON, VA – Government officials are considering significantly greater prison time for perpetrators of identity theft crimes that involve U.S. infrastructure systems or computers associated with U.S. national security. The U.S. Sentencing Commission is the entity responsible for reviewing and updating penalties in this area. Public comments are due by March 30.

The move toward stronger penalties reflects a growing realization by the federal government that ID theft is no longer merely a nuisance but a crime with potentially devastating economic and national security implications, according to Lee Zeichner, president of Zeichner Risk Analytics (ZRA).

*“The government is finally beginning to acknowledge that addressing cyber crimes is a grave matter of economic security.” said Melissa Grondin, Director of Information Assurance at ZRA. “Higher penalties signal a profound change in the federal government’s approach toward cyber crime.”*

As companies and government agencies rely increasingly on computer networks for their daily operations, the opportunities for unauthorized access are vast. Perpetrators are using more sophisticated techniques that threaten even the most state-of-the-art security protections available for computer networks. Perpetrators are also targeting larger, more lucrative institutions, such as retail giants and government agencies, which can impact far more people and incur greater economic losses in one pass. In 2006, when perpetrators hacked the unsecured databases of retail giant TJ Maxx, they accessed more than 45 million credit and debit card numbers and the company incurred \$5 million in its fourth quarter to cover costs of containment and investigation.

In spite of this trend, however, the prison sentences for identity theft crimes are often not commensurate with rising levels of economic damages. Just earlier this week, a federal judge issued a four-year sentence for a convicted hacker, even though the hacker was eligible to serve up to 60 years in prison. According to the Federal Bureau of Investigations, the perpetrator incurred more than \$20 million in losses after infecting up to 250,000 computers and stealing the identities of thousands of people.

*(Continued on Page 2)*

Press Release (Cont. from 1)

5 Crimes

Under the Identity Theft Enforcement and Restitution Act of 2008,<sup>1</sup> the U.S. Sentencing Commission is responsible for reviewing its current penalties and amending them to reflect the seriousness of computer-based crimes. The Commission is an independent body of the judicial branch responsible for setting guidelines for federal judges when determining sentences for all types of crimes.

The five major cyber crimes under review are:

- Fraud Related to Identification Documents, Authentication Features and Information;
- Aggravated Identity Theft;
- Fraud Related to Computers;
- Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited; and
- Unlawful Access to Stored Communications.

Factors for Enhancing/Reducing Penalties

The Commission assigns a base offense value to each crime, ranging from 1 to 43, which guides judges when sentencing convicted criminals. The more serious the crime, the higher the base offense level. A crime at Offense Level 1, for example, calls for a prison sentence of 0 to 6 months, while a more serious crime at Offense Level 43 calls for 'life in prison'. Factors that can further increase or decrease the offense value include criteria such as whether the crime:

- Disrupted a critical infrastructure system;
- Involved a computer used for U.S. national security or defense;
- Resulted in potential and actual loss (including the value of the information);
- Among other 10 additional factors (see attached ZRA brief).

As the Commission reviews its cyber crime penalties, it is seeking input, through the end of March, from private-sector executives, agency officials and others on how best to amend them. Intense debate in upcoming months will focus on how much stronger the penalties should be. Judicial hard liners will have the opportunity to push for far stiffer penalties, giving federal judges the tools to throw the book at cyber criminals in the current economic climate. ❖

\*\*\*\*\*

About Zeichner Risk Analytics

Zeichner Risk Analytics is the leading provider of risk and security governance analysis for business and trade professionals. Our vision is to be a trusted and valued source of integrated regulatory and business analysis that supports critical business assurance goals. As a corporate consulting business, we are

(Continued on Page 3)

<sup>1</sup> "Congress Attacks CyberCrime on Several Fronts," Zeichner Risk Assessment, Vol. 1, No. 27, September 29, 2008 ([http://www.zra.com/docs/ZRA\\_Newsletters/ZRA\\_092908.pdf](http://www.zra.com/docs/ZRA_Newsletters/ZRA_092908.pdf)).

Press Release (*Cont. from 2*)

focused on helping clients understand the security requirements of the 21st century and find effective business process solutions to risk management, corporate governance, and new regulatory impacts.

ZRA has extensive expertise covering data management and security directly with Chief Executive Officers (CEOs) from mid-to-large, market-cap public companies that operate globally. ZRA has published findings derived from working with CEOs, including strategic risk frameworks, collections of regulatory materials, and risk checklists. From HIPAA and healthcare to ID theft and finance, ZRA has the knowledge your business needs to stay in compliance without diverting focus from your business goals.

*For more information on this issue, please contact Melissa Grondin ([mgrondin@zra.com](mailto:mgrondin@zra.com)).*