

**TESTIMONY BEFORE THE
GOVERNMENT REFORM SUBCOMMITTEE
ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL
RELATIONS AND THE CENSUS**

U.S. HOUSE OF REPRESENTATIVES

September 22, 2004

**By Howard A. Schmidt
Chief Information Security Officer, eBay Inc.**

Introduction

Chairman Putnam, Ranking Member Clay, distinguished members of the Committee; my name is Howard A. Schmidt. I am the Vice President and Chief Information Security Officer for eBay, where I lead a team responsible for ensuring the trustworthiness and security of the services that bring so many global citizens together in a vast global marketplace each day. I would like to thank you for the opportunity to come before this important Subcommittee as well as your continued leadership on cyber security issues. Prior to my current position at eBay, I had the privilege of being appointed by President Bush, along with Richard Clarke, to lead the President's Critical Infrastructure Protection Board, which represented one part of the overall governmental response to the threat of cyber security attacks in the wake of September 11. I retired from 31 years of public service after completing and publishing the "National Strategy to Defend Cyberspace," working with a team of dedicated public servants, this distinguished body and the American public.

I have had the privilege of working with committed individuals in the private sector, law enforcement, and government to forge the collaboration and cooperation that is so essential to safeguard cyber space for everyone, from inexperienced home users to large well-run corporate enterprises. I assisted in the formation of some of the first collaborative efforts in the law enforcement community to address cyber crime with local law enforcement, the FBI, Secret Service and the dedicated military criminal investigators. I also helped lead the creation of the Information Technology Information Sharing and Analysis Center (IT-ISAC) and had the honor of serving as its first President.

I continue to proudly serve in the U.S. Army Reserves, assigned to the 701st MP Group, (CID) as a Special Agent with the computer crime unit at CID headquarters. I also serve on the Board of Directors for (ISC)², the body that oversees certification of security professionals through the CISSP certification. And, I serve on the Information Security Privacy Advisory Board, appointed by the Secretary of Commerce to advise NIST, CSD and OMB.

The challenges of identity theft and ID management

My remarks today will focus in three areas: 1) how eBay has been one of the leaders on the issue of online identity theft and “phishing,” a growing threat to consumers, businesses, federal employees and basically anyone who uses the Internet; 2) an overview of some of the industry wide efforts that have been undertaken to combat online ID theft; and 3) a discussion of some steps that the public and private sector can work on to move forward in providing online identity management.

You have probably heard some of the numbers before. The U.S. Federal Trade Commission (FTC) reported earlier this year that identity theft topped the list of consumer complaints for the fourth year in a row. Unfortunately, online fraud accounted for a large number of these complaints. The FTC received 33 percent more identity theft complaints in 2003 compared with 2002, and Internet fraud accounted for 55 percent of all fraud complaints, up from 45 percent in 2002. These numbers alone don’t tell the full story. According to a June 2004 Forrester Research report, nine percent of U.S. online consumers – 6 million households that use the Internet – have experienced identity fraud.

What’s both interesting and troublesome about the numbers that I just mentioned, including the large number of households that have been victimized by online criminals, is that the numbers reported by the FTC next year are likely to be worse if we do not take action now. Why? One major reason is the explosion in phishing scams on the Internet. Phishing, or the use of fake e-mails and Web sites to steal bank account and other sensitive information such as social security numbers, has “hoodwinked” millions of victims globally. The criminals send thousands of emails telling people that there is an error with their online account and ask them to fill in an “update form” or their account will be closed. This form has the look and feel of major e-commerce sites – there was even a fake email from someone pretending to be the FBI and the FDIC asking unsuspecting users to enter personal information into a fake web site or their bank account would be closed. While online criminals have been busy, they have also been quite successful.

Although this appears to be a recent phenomenon, identity theft is a very old type of crime. The “phishing” email is but a new twist to an old scam. In the mid 1980s we taught classes at the Federal Law Enforcement Training Center on a technique called carding, where individuals would “shoulder surf” people’s credit and calling cards at airports and train stations, then distribute them worldwide via “Computer Bulletin Boards.” Dumpster diving still is an effective method for individuals to obtain personal information and is used regularly to create false identities. Hacking into systems and stealing personal information is yet another way this disturbing trend is continued. As we get better at securing our systems, as online security improves, the next “soft target” the cyber criminals go after are the end users, relying on age old methods involving scams and deception. This is the basis of what “phishing” is all about. Some of the first instances of what we now call “phishing” started over 5 years ago when individuals sent fake emails reporting a problem with an account, and presented a “form” to fill out and

“fix” the account. The initial intent was to steal online time from legitimate users for criminals’ use. This has since changed to be mainly a financial motive.

According to a June 2004 study by Gartner, nearly 2 million people reported that their checking accounts were breached in some way during the last year. In a May 2004 study, Gartner reported that a staggering 57 million online users in the United States alone had received a “phishing e-mail during the prior year. Gartner reports that direct losses from identity theft fraud as a result of “phishing” attacks – including new account, checking account and credit card account fraud – cost U.S. banks and credit card issuers about \$1.2 billion last year. These numbers are likely just the tip of the iceberg and the impact on our economy as well as our pocketbooks is considerable.

Why are consumers and businesses being duped? Well, many of the reasons tie into social engineering. But, not all of them. Heightened awareness alone will not stop “phishing”. Better cyber hygiene is surely a part of the solution, but it is only one important part. The reality is, as more people become aware of current “phishing” scams, the cyber criminals often get even more clever, and create new, more sophisticated techniques. One example of an emerging threat in phishing is what a colleague at Indiana University calls “context aware” “phishing” attacks. These attacks are mounted using messages that are somehow expected (or even welcomed) – from their context – by the victim. Markus Jakobsson, who started his analysis of this problem while a Principal Research Scientist at RSA Security Laboratories in Massachusetts, states that initial analysis of context aware attacks indicate a success rate of close to 50 percent. *Note: See “Modeling and Preventing Phishing Attacks” by Markus Jakobsson, School of Informatics, Indiana University at Bloomington.

Corporate enterprises such as eBay are continually enhancing security. But new threats require continued education of the end-user, technology improvements, information sharing and analysis to reduce the impact of these threats. eBay has developed advanced applications to identify potential spoofed/”phishing” web sites and has established a full time team dedicated to identifying and taking down these spoofed/”phishing” sites as well as notifying other companies when spoofed sites are discovered. Working with our partner Whole Security, Inc. eBay has also created an account guard feature within the eBay toolbar that turns green when on an eBay or PayPal site, and turns red and displays a dialogue box identifying it as fraudulent if one goes to a phishing site. If an eBay password is used on a site that is not eBay, the account guard feature displays a dialogue box stating that it is not a good practice to use the same password for multiple web sites. eBay continues to work with other industry leaders looking for long term solutions to identify theft and “phishing.”

What Can Consumers and the Public and Private Sector Do?

The widespread success of current phishing and other kinds of online fraud combined with criminals constantly coming up with more sophisticated ways to scam, means that Internet users have to do more. One critical first step is authentication. While

putting together the *National Strategy to Secure Cyberspace* I emphasized that authentication had to be included. “A/R 4-2: Through the ongoing EAuthentication initiative, the federal government will review the need for stronger access control and authentication; explore the extent to which all departments can employ the same physical and logical access control tools and authentication mechanisms; and, consequently, further promote consistency and interoperability.”

Think about it. To know that you are you is really important to your online commerce auctioneer, your online store, your bank, your DMV, your online pharmacy, the IRS...you get the picture. And, if you think about it some more, strong or two-factor authentication methods are the best way to protect your identity and your personal, business, or government agency information. When drafting the *National Strategy to Secure Cyberspace* the concept of strong online authentication was not viewed as a Homeland Security issue by some offices within the government. But I contend that it is a Homeland Security issue. The lack of strong online authentication allows an individual's private information to be accessed by unauthorized persons who can then take over that individual's good identity. Computer systems can also be taken over and used in concert with thousands of others to launch distributed denial of service attacks. In recent past law enforcement has seen instances of more than 15,000 broadband connections being hijacked and turned into a remote (bot) network. In many instances end-user machines used for remote access into corporate networks can be compromised, thus also providing a gateway into critical infrastructure. As we get better at protecting physical identification, the next logical place for terrorists and organized criminals to obtain identities is online. We can prevent this by implementing strong two factor authentication.

With the new threats we have seen increasing online, passwords will need to evolve into a more strong method of authentication in the future. Passwords that are easy to remember can be easily guessed by hackers, and passwords that are more complicated have to be written down, making them more vulnerable to thieves. Do you or members of your family use the same easy-to-remember password at multiple sites online? Do you or your employees write your password on a piece of paper and put it under your mousepad at work? These are pretty common mistakes and even users that are generally more cyber security aware sometimes make them out of convenience.

We have created a system where we must use complex passwords to login to various systems. We also have to change those passwords frequently creating another challenge for mere human beings to remember these complex passwords. This is made even worse by the need to use different passwords for different systems that few people voluntarily choose to do. This is a known weakness often exploited by criminal hackers.

The government can be a leader in accelerating the creation of digital identity management that would work for government services as well as online e-commerce. The nation could be well served to have two-factor authentication in place by the end of 2005. The DoD has moved this process forward through their Combination Access Card (CAC). Many federal agencies and even security conscious legislatures, including the House of Representatives, use Secure ID smart tokens from the identity and access

management provider RSA Security for remote logical access. The President's Homeland Security Directive on August 27th that establishes a "Policy for a Common Identification Standard for Federal Employees and Contractors" has significantly elevated the use of federal identities as a federal government priority. The Directive requires the new standard being developed by the National Institute for Standards and Technology be implemented by the end of November 2005.

Consumer facing companies have an important role to play as well. My company, eBay, constantly educates consumers about the importance of authentication as well as good cyber hygiene. We believe that we are one of those forward-thinking companies that get it and will continue to offer our users more and more solutions to combat identity theft and other online threats. I am a great believer that federated identities can be recognized as easily as a driver's license, military ID or passport with the extra feature of instant validation online. One example of using federation is to have the ability to log onto my organization's network while using the same federated identification to do my online banking or shopping online from overseas.

Consumers are demanding more security and key players are stepping up to the plate. Companies such as RSA Security, Entrust, GeoTrust and Verisign have been leading this charge for a number of years and now provide solutions for improved identity management not available in the past. Recently a major ISP and RSA Security announced that strong authentication devices will now be available to millions of consumers through an easy to use subscription service. This is a major development and I anticipate that more and more ISPs, banks and other businesses will be taking this very important step in the coming months and years. Consumers benefit, businesses benefit – we all benefit. Criminals lose.

In addition to offering specific solutions, industry is coming together in various groups to educate the public, share information, discuss emerging threats, and address public policy issues related to phishing and other online fraud. We worked with the Information Technology Association of America (ITAA) to pull together a number of providers and vendors – including eBay – to form the Anti-Online Identity Theft Coalition. The Coalition has four major goals: 1) to build technology to reduce the likelihood of these mails ever reaching their intended victim; 2) to provide awareness training to consumers so they can more readily identify these criminal acts; 3) to share information on new scams amongst the various security teams; and, 4) to insure accountability by working with law enforcement to identify and prosecute these bad actors.

The Anti-Phishing Working Group has become a one-stop shop for information on "phishing". Many organizations – public and private – share information within the group about current and evolving threats. The financial services industry has an important anti-fraud working group at BITS and the Financial Services Technology Consortium has a counter-phishing initiative. The National Cyber Security Alliance is a public-private partnership spearheading efforts to educate consumers and small businesses on cyber security and protection from online identity theft.

Another organization working on identity management is the Electronic Authentication Partnership (EAP). This group is a multi-industry partnership working on the vital task of enabling interoperability among public and private electronic authentication (e-authentication) systems. Interoperability of e-authentication systems is essential to the cost-effective operation of safe and secure systems that perform essential electronic transactions and tasks across industry lines.

I have also had the distinct pleasure of working with Commissioner Orson Swindle of the Federal Trade Commission, who has been a beacon of light for the protection of consumers' privacy and security. With his help in the creation of the FTC's "Dewey" program and his tireless support for town hall meetings, he has truly fostered a greater "culture of security" globally.

Role of Cyber Crime Investigations

The Department of Justice (DoJ), the U.S. Secret Service and the FBI have significantly decreased their response times and increased the priority of cyber crime investigation. FBI Director Mueller has placed cyber crime as a top five priority of the FBI, and the Secret Service has added a number of electronic crime task forces to investigate and prosecute cyber criminals. All of DoD's criminal investigative organizations are leaders in investigating cyber crimes and include among their ranks some of the best investigators in the world. DoJ, through its Computer Crime and Intellectual Property Section, has chaired the G-8 Subcommittee on cyber crime and has been a significant driving force in combating cyber crime worldwide.

For the past three years, we have seen a significant increase in the number of cyber crime investigations undertaken by all levels of law enforcement, federal, state, local and international. Although we have had success in a number of investigations, I would recommend to the Committee to look again at the federal agencies and their coordination and investigative responsibilities.

Just two weeks ago, the Department of Justice announced Operation Slam Spam in which the private sector, law enforcement, the National White Collar Crime Center and the Internet Crimes Complaint Center took dramatic steps against those that would continue to attack our online personalities. I am assured that this will not be the only strike against those that affect the way we work, play and enjoy the online world.

Conclusion

Despite these and many other efforts, solutions, and security enhancements, we can be certain that the nature and sophistication of online fraud and "phishing" scams will evolve. To combat this evolution we need to quickly move to a world where strong identity is the standard and where we have a greater assurance that we can choose any type of a device, whether it is a smart card device, an RSA secure ID device or a USB device, and we can use it for government and e-commerce.

Finally, we must recognize that cyber security is no longer merely about products, services and strategies to protect key operations. What is at stake in the effective implementation of advanced cyber security technologies and strategies is nothing less than the ability to unleash the next wave of information technology-led growth in jobs and productivity. Cyber security is an essential enabler to the advent of the next generation Internet and all it holds for how we work, live, and learn.

I thank you once again for the opportunity to appear before this distinguished committee and I look forward to any questions that you might have.

Biography of Howard A. Schmidt

Howard A. Schmidt joined eBay Inc. as Vice President and Chief Information Security Officer in May of 2003. He retired from the federal government after 31 years of public service. He was appointed by President Bush as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House in December 2001. He assumed the role as the Chair in January 2003, until his retirement in May 2003.

Prior to the White House, Howard was chief security officer for Microsoft Corp., where his duties included CISO, CSO and forming and directing the Trustworthy Computing Security Strategies Group.

Before Microsoft, Mr. Schmidt was a supervisory special agent and director of the Air Force Office of Special Investigations (AFOSI), Computer Forensic Lab and Computer Crime and Information Warfare Division. While there, he established the first dedicated computer forensic lab in the government.

Before AFOSI, Mr. Schmidt was with the FBI at the National Drug Intelligence Center, where he headed the Computer Exploitation Team. He is recognized as one of the pioneers in the field of computer forensics and computer evidence collection. Before working at the FBI, Mr. Schmidt was a city police officer from 1983 to 1994 for the Chandler Police Department in Arizona..

Mr. Schmidt served with the U.S. Air Force in various roles from 1967 to 1983, both in active duty and in the civil service. He had served in the Arizona Air National Guard from 1989 until 1998 when he transferred to the U.S. Army Reserves as a Special Agent, Criminal Investigation Division. He has testified as an expert witness in federal and military courts in the areas of computer crime, computer forensics and Internet crime.

Mr. Schmidt had also served as the international president of the Information Systems Security Association (ISSA) and the Information Technology Information Sharing and Analysis Center (IT-ISAC). He is a former executive board member of the International Organization of Computer Evidence, and served as the co-chairman of the Federal Computer Investigations Committee. He is a member of the American Academy of Forensic Scientists. He serves as an advisory board member for the Technical Research Institute of the National White Collar Crime Center, and is a distinguished special lecturer at the University of New Haven, Conn., teaching a graduate certificate course in forensic computing.

He served as an augmented member to the President's Committee of Advisors on Science and Technology in the formation of an Institute for Information Infrastructure Protection. He has testified before congressional committees on computer security and cyber crime, and has been instrumental in the creation of public and private partnerships and information-sharing initiatives.

Mr. Schmidt has been appointed to the Information Security Privacy Advisory Board (ISPAB) to advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST.

Mr. Schmidt holds a bachelor's degree in business administration (BSBA), a master's degree in organizational management (MAOM) and an honorary Doctorate in Humane Letters from the University of Phoenix.