

Statement of Bill Conner
Chairman, President and CEO
Entrust, Inc.

Before
The House Government Reform Committee
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census

“Identity Theft: The Causes, Costs, Consequences, and Potential Solutions”

September 22, 2004

Good Morning. Chairman Putnam and Members of the Subcommittee, thank you for the opportunity to provide testimony on this important and timely subject. My name is Bill Conner, and I am Chairman, President and CEO of Entrust, Inc. In my testimony today, I will address the threat of identify theft and phishing and examine what Congress can do about it.

I want to be very clear in my message. Identity theft and phishing are serious problems that threaten not only to undermine trust in business and the Internet, but also to disrupt our national economy. They are not isolated issues that can be tackled by themselves, but part of the broader cyber security challenge facing the networked economy.

Although some companies have recognized the importance of cyber security to their business, most are struggling with it. It is incumbent on this Subcommittee to galvanize government and industry to implement strong cyber security programs.

Entrust is a world leader in securing digital identities and information. Over 1,200 enterprises and government agencies in more than 50 countries use our security software solutions, so we have a good perspective on today's cyber security reality. As a company, we are leading the evolution from defensive-oriented security technology approaches to a more proactive business security strategy that not only protects information assets, but also enables business needs. This strategy involves creating a more robust, manageable business security environment through the use of technologies such as encryption, digital signatures, authentication and authorization. Our mission is to

work with customers to put in place the technologies, policies and procedures necessary to protect digital identities and information.

Over the past two years, I have co-chaired two major cyber security task forces: 1) the Business Software Alliance Task Force on Information Security Governance, and 2) the National Cyber Security Partnership Task Force on Corporate Governance. Through this work and my professional experience at Entrust, I have become convinced that the only way for enterprises to address cyber security is to elevate the issue to executive management with board oversight within an information security governance framework. Although Congress has passed several cyber security bills in recent years, each addresses only one facet of the problem. Because cyber security is a constantly moving target, I do not believe that this piecemeal approach will be successful. Only by treating cyber security as a governance issue and adhering to a specific information security governance framework for employees at all levels, can organizations truly make sustained progress.

I. What are identity theft and phishing, and why are they such serious problems?

Just as the Internet has supercharged commercial transactions, so has it heightened the potential for cyber crime. Identity theft is an especially pernicious form of cyber crime, and phishing is an especially potent form of identity theft. Identity theft consists of stealing a corporation's or individual's identity and using it for illegal purposes. Phishing consists of using "spoofed" e-mails and phony websites to fool recipients into divulging sensitive personal financial information, such as credit card numbers, social security numbers and passwords. By masquerading as reputable companies, phishers have

already lured up to 5% of recipients to respond to their false representations, and this crime is still in its infancy.

Over the past decade, consumers, enterprises and governments have become increasingly dependant on the Internet. What began as an easy way to communicate and access information has evolved into a means of conducting on-line transactions, integrating strategic relationships and managing customer accounts. Unfortunately, as critical applications and sensitive information have moved onto the Internet, security has not kept pace. As a result, many consumers and businesses are walking in a dangerous neighborhood and don't even know it. A few statistics demonstrate the seriousness of the problem.

- The US Federal Trade Commission has highlighted identity theft as the fastest growing white collar crime in America with annual losses of \$9 billion in 2003. Computer Economics, a technology consulting firm, estimates that losses will grow to over \$16 billion by the end of 2004.
- According to Forrester Research, 9% of US online consumers (an estimated 6 million households) have experienced identity theft.
- Industry associations report that phishing attacks are now growing at over 50% per month.

Despite these alarming statistics, many consumers still don't understand the problem, and business has been slow to address it. Part of the problem is that phishing attacks are becoming more and more sophisticated. Today's scams are like counterfeit money – they

are so carefully rendered that many consumers believe they are legitimate and therefore provide sensitive information freely. The biggest barrier to progress, however, is the business mindset about cyber security. Despite the fact that businesses face serious financial risks from identity theft and phishing, most companies take inadequate cyber security precautions.

II. What is the Market Response?

The market response falls into three categories: 1) Do nothing; 2) Take limited precautions; and 3) Attack the problem internally and externally. Each of these is examined below.

Do Nothing

Too many companies continue to ignore the problem, pretending that it doesn't exist, or if it does, that it won't have an impact on them. According to *The State of Information Security, 2004* (a worldwide survey of more than 8,100 IT security professionals in 62 countries compiled by CIO Magazine and PricewaterhouseCoopers), 8% of organizations admit that they have no formal security policy, and the real number is probably higher. There are many reasons for this failure to take action.

1. *They don't know what to do.* Despite the fact that identity theft and cyber crime are growing exponentially, many companies are still unaware of them. For example, in our discussions with a Fortune 500 health care provider during the past few months, we were surprised to learn that their CIO had never heard of

phishing. Even when companies are aware of the problem, they often resist taking action because of concern about inconveniencing their customers. For example, a major bank realized that it did not have adequate cyber security protections to securely authenticate its sensitive communications, but was unwilling to accept any solution that required more than a few milliseconds response time for authentication during fail-over. Since no security products met this standard, the bank was unwilling to implement a solution. In the absence of a clear course of action, many firms are waiting for others to take the lead. This behavior has created a “chicken-and-egg” conundrum -- everyone knows there is a problem, but they won’t act aggressively until others do.

2. *It’s not a corporate priority.* Many firms are unwilling to elevate identity theft (and the need for a cyber security program that it implies) to the attention of senior management. *The State of Information Security, 2004* reports that 20% of IT security professionals cite limited support from executives as a barrier to good security. This statistic indicates that many organizations continue to treat cyber security primarily as a technical issue that can be delegated to the CIO, not as a governance issue that requires the attention of boards, CEOs, and business unit heads. This failure to make cyber security a corporate governance priority often leads to a failure to implement solutions. All too often, even when organizations do buy technology to secure their operations, they never fully deploy it because there is no plan or connection back to their business needs. Federal agencies are only too familiar with this problem.

3. *Government regulations are unclear.* A raft of legislation has been passed in recent years that addresses cyber security issues, including the Financial Modernization Act (Gramm-Leach-Bliley), the Health Insurance Portability and Accountability Act (HIPAA) and California Senate Bill 1386. Section 404 of the Public Company Accounting Reform and Investor Protection Act (Sarbanes-Oxley), with its focus on appropriate “internal controls” for financial information, also raises questions about cyber security. Each of these laws addresses different aspects of the problem, and each is the subject of extensive debate. Until there is better understanding of what it takes to comply with these laws and the penalties for failure to do so, progress will be slow.

4. *Technology vendors aren't doing enough.* Many enterprises and consumers criticize technology vendors for producing poor quality products with security holes that require constant patching. Others blame vendors for over-hyping their solutions, failing to connect them to business needs, and ignoring ways to measure return on investment. Still others fault the complexity of the technology itself. Vendors are working to respond to these criticisms since they understand that cyber security technology must be more closely integrated with applications and easier to deploy and use if it is to be widely embraced.

Take Limited Precautions.

Most companies fall into this category. They know that they must do something to satisfy customer expectations, but are worried about any inconvenience that may result.

Similarly, they know they must meet government regulations, but are confounded by the vagaries of current legislation. Even when they do take action, they are reluctant to speak openly about it out of concern that doing so will increase their liability and make them a target for hackers. According to *The State of Information Security, 2004*, over half of IT security professionals are not reporting breaches at all. These organizations tend to do lots of studies, pilots and tests. They may deploy some technology around the margins that is easy to implement, but never commit to implementing a robust cyber security solution. Keeping out of trouble with management and doing just enough to satisfy regulators seems to be the goal, not implementing solutions that are based on careful risk analysis and that address business needs.

Attack the problem internally and externally.

Very few companies have made cyber security a corporate governance priority by linking it to their business needs, implementing strong internal controls, and focusing public attention on the issue. Those that have tend to be banks, on-line retailers, companies in the cyber security industry or organizations that have experienced significant breaches.

These companies do not view cyber security as an isolated problem that can be addressed once and forgotten. Nor do they view it as a consumer problem. Instead, they embrace it as a core business issue that requires continuous vigilance and sustained progress, much like quality assurance. Even these organizations, however, still have a long way to go. I

can speak from personal experience here, because even though Entrust has had an information security governance framework in place for two years, we still have a lot of work ahead of us. Cyber security is a journey, not a one-time event, and policies must be systematically reviewed, measured and refined. Even when companies do implement cyber security programs, they often fail to follow up with the proper oversight. According to *The State of Cyber Security, 2004* only a little over one-third of organizations with cyber security policies have measured and reviewed them.

I believe that the road to information security lies through corporate governance. If the government and the private sector are to make significant progress securing their information assets, executive management must make information security an integral part of core business operations. There is no better way to accomplish this goal than to highlight it as part of the internal controls and policies that constitute corporate governance and create a framework that defines tasks for employees at all levels of an organization.

There is a lot of consumer data that supports the wisdom of an aggressive cyber security program.

- According to a survey that Symantec conducted with InSightExpress, over 40% of consumers are very concerned about online fraud, and the majority of respondents have changed the way they use the Internet because of their concerns. About 32% of them won't use the Internet for online banking, and almost 15% say they don't trust the Internet.

- Worry about identity theft is even more acute among online users. According to Forrester Research, 61% of online consumers are extremely or very concerned about it.
- According to research commissioned by Entrust, 80% of Internet users are worried about someone stealing their on-line identity and using it to access their on-line bank accounts. Importantly, 72% of them would use online banking if online identity security was improved. And 90% of existing online bank users would take advantage of additional, higher value services if their online identities were better protected.
- One-in-five user-name/passwords is breached. According to Entrust's research, most Internet users would be willing to change their habits to better protect their identity. For example, 78% would be willing to use a second factor of authentication when accessing their bank accounts to improve the security of their identity.

IV. What are the lessons?

We can draw several lessons from the threat that identity theft and phishing pose. These lessons, in turn, point the way to constructive Congressional action.

- Identity theft and phishing are extremely serious problems that, left unchecked, have the potential to undermine many e-commerce and e-government applications that depend on trust in the Internet.
- They are not isolated problems, but part of the broader cyber security challenge.

- Current laws tend to treat cyber security as a secondary issue. As a result, they cite requirements that are vague and don't do enough to advance understanding of the costs and benefits that are necessary for industry to orchestrate an effective response.
- The private sector has not taken action sufficient to address the problem and is still reluctant to talk openly about it.
- Companies must build better products. Entrust and others are doing just that, and soon will have new solutions that are inexpensive and suited to the mass market.
- Technical solutions alone are not enough. They must be coupled with information security governance programs that make cyber security an integral part of the on-line experience.
- Education is important, but by itself is insufficient since it assumes that the problem rests with consumers, not with business.

V. What is the role of Congress?

Congress has a vital role to play in addressing the related threats of identity theft and phishing. Its number one priority should be to create a bright line between acceptable and unacceptable behavior. As long as this line remains fuzzy, the market will be caught in a cyber security paradox – everyone knows that it is a serious problem, but in the absence of clear solutions or penalties they are waiting for someone else to take the lead.

As mentioned earlier, it is difficult to address phishing and identity theft in isolation since they are part of an overall cyber security problem. Recognizing that fact, I would like to offer the following recommendations for consideration by the Subcommittee:

1. **Congress should demand that Federal agencies purchase *and deploy* cyber security technologies.** Although Federal agencies purchase a lot of technology to secure their information assets, they often fail to deploy it fully. This issue is especially relevant for this Subcommittee since you have jurisdiction over technology and information policy for the Federal government. Mr. Chairman, as part of your oversight of the Federal Information Security Management Act (FISMA), I would urge you to initiate a dialogue about how to drive implementation of cyber security technologies that Federal agencies have purchased but not fully implemented. As part of this discussion, you should examine how both carrots and sticks can accelerate deployment.
2. **Congress should stipulate that cyber security measures are an explicit part of Section 404 of the Sarbanes-Oxley bill.** Section 404 of Sarbanes-Oxley requires senior management of publicly traded companies to establish and maintain adequate internal controls for financial reporting and to assess the effectiveness of these controls annually. It does not mention cyber security, but it is hard to escape the conclusion that publicly traded companies cannot protect their financial information (most of which is kept in digital form) without employing some sort of cyber security. This lack of specificity adds to the confusion

surrounding private sector efforts to secure digital identities and information. By stipulating that Section 404 of Sarbanes Oxley applies to cyber security controls, Congress could encourage publicly traded companies to make information security to a corporate governance priority.

3. **Congress should drive implementation of the Homeland Security Presidential Directive HSPD-12.** This Directive is designed to provide Federal employees with digital credentials that provide strong authentication and can be used to secure identities, information and transactions. The key to effective deployment is to integrate these credentials with new and existing applications. Unless this integration is done without significantly revising existing applications, these credentials will just sit on a shelf. Just as this Subcommittee has effectively used FISMA to drive Federal implementation of cyber security programs, so should it use HSPD-12 to grade and discipline the roll-out of digital credentials. Doing so would accelerate implementation, provide for consistent delivery and spur immediate usage. The capability to issue these digital credentials already exists in many Federal agencies, and by linking architecture with applications Congress could help spur the Federal E-authentication program.

4. **The Federal government should lead by example.** Congress should discourage Federal agencies from purchasing products from companies with inadequate cyber security programs or a record for poor quality. Congress should also create incentives for companies that institute robust information security governance

programs. An example of such a program can be found in the report, Information Security Governance: A Call to Action, that was release by the National Cyber Security Partnership Task Force on Corporate Governance in April 2004. To be effective these information security governance programs should be regularly reviewed, measured and updated.

The identity theft and phishing epidemic shows that the cyber security threat is real and has the potential to incapacitate the Internet. The private sector has been slow to respond to the problem, and Congress should consider ways to spur a more constructive market response.