TESTIMONY OF

Michael Barrett
Vice President, Information Risk Management
Chief Information Security Officer
PayPal
eBay Inc.

BEFORE THE
United States House of Representatives
Committee on Science, Space and Technology
Subcommittee on Research and Subcommittee on Technology

"Cyber R&D Challenges and Solutions"

PRESENTED
Rayburn House Office Building, Room 2318
February 26, 2013
10:00 AM

Testimony of

Michael Barrett

Vice President, Information Risk Management

Chief Information Security Officer
PayPal

eBay Inc.

Before the

United States House of Representatives

Committee on Science, Space and Technology

Subcommittee on Research and Subcommittee on Technology

"Cyber R&D Challenges and Solutions"

***Presented*:**

Rayburn House Office Building, Room 2318

February 26, 2013

10:00 AM

Chairman Bucshon, Chairman Massie, Ranking Member Lipinski, Ranking Member Wilson, and Members of the Subcommittee: Thank you for the opportunity to testify today about PayPal and what we, and the eBay Inc. family are doing to protect our users from the growing cybersecurity challenges that are facing Internet-enabled companies large and small and what our nation's policymakers can do to assist us in tackling this growing problem.

My name Michael Barrett and I am the Vice President of Informational Risk Management and Chief Information Security Officer for PayPal, a member of the eBay Inc. family. Founded in 1995 in San Jose, Calif., eBay Inc. connects millions of buyers and sellers globally on a daily basis through eBay, the world's largest online marketplace, and PayPal, which enables individuals and businesses to securely, easily, and quickly send and receive online

payments. We also reach millions through specialized marketplaces such as StubHub, the world's largest ticket marketplace, and eBay classifieds sites. And through our company GSI Commerce, eBay Inc. has become the leading provider of eCommerce and interactive marketing services for many of the world's premier brands and retailers, such as Toys R Us, Ralph Lauren and Dick's Sporting Goods.

Additionally, eBay Inc. is actively working to revolutionize global commerce with the recent additions of mobile technology companies WHERE, Milo, Zong and others combined with the seasoned services of eBay Marketplaces Mobile and PayPal Mobile. In fact, in 2012, eBay Inc. generated nearly $14 billion in global mobile sales. PayPal Mobile also experienced great popularity across the globe, with over 17 million consumers in over 80 markets worldwide. Our global consumers bought everything from cars, clothing, shoes, electronics, and toys from eBay and PayPal's mobile applications.

eBay Inc. is a very diverse family of businesses supporting millions of users ranging from individual consumers to merchants and retailers of every shape and size. As enablers of commerce, eBay Inc. and PayPal facilitate consumers buying just about anything whether on or offline. We enable consumers to pay online, pay with a phone, pay with a card from your wallet or pay with nothing but a phone number and a secure pin. All sustainable 21st Century retail business models, large and small alike, will use the Internet and mobile technology tools and it is our hope to be their partner in that venture.

With this growing trend in mind, eBay Inc. and PayPal recognize that our success and the success of our retail partners are dependent on our ability to engender consumer trust and confidence. It is our belief that without trust, the Internet and mobile marketplaces will fail to reach their full potential. Security and trust are mutually reinforcing. It is hard to build consumer trust without ensuring the safety and security of a consumer's personal information, whether it is financial data, transaction history, etc.

To foster that trust, we've worked to meet customer expectations with every product we offer. PayPal and its "shop without sharing" design, was created to offer a secure alternative to

traditional payment systems. Security is one of the fundamental building blocks of the PayPal services. The beauty of PayPal is that it allows consumers to send money or pay for a good or service without ever having to expose their credit card or bank account information to merchants or other PayPal users. It allows consumers to shop online or on their mobile device without having to share the most sensitive personally identifiable information, financial and banking information. Not only does this security-enhancing technology allow consumers to fully enjoy the convenience of online and mobile commerce without worrying about safety and security concerns, but it also allows merchants to receive payments without the cost and potential liability associated with processing and securing financial information.

However, as the Internet and mobile platforms become more attractive to consumers and businesses alike, it also attracts criminals and bad actors that are looking to profit by exploiting Internet companies and users. And unfortunately, their behavior has furthered the perception of certain individuals that the Internet and mobile platforms are unsafe and therefore unsuitable for everyday use. Companies like eBay and PayPal will continue to fight back against this perception and work to protect the safety and security of our platform and our users. However, as cybercriminal activities slowly get worse, we believe that traditional technical measures alone cannot significantly move the trend line in a positive direction and that there are concrete steps that industry and policymakers should take to significantly mitigate the impact of cybercrime and reduce its frequency.

I would like to take the next few minutes to highlight some of the successful security-related programs that my team has engaged in over the last few years and also recommend some areas that would benefit from government engagement.

PayPal's Efforts on Cybersecurity

DMARC: Domain-based Message Authentication, Reporting & Conformance

On a daily basis, Internet companies, including PayPal, run into sites that have been compromised and are being used as "phishing" or "spoof" sites, which are intended to defraud

Internet companies and their users by various means. With the rise of the social Internet and the ubiquity of e-commerce, spammers and phishers have a tremendous financial incentive to compromise user accounts, enabling theft of passwords, bank accounts, credit cards, and more. Unfortunately, email is very easy to spoof and criminals have found this activity to be an opportunity to exploit user's trust of well-known brands. By simply inserting the logo of a well-known brand into an email, spoofers give their emails instant legitimacy with many users.

Recognizing the growing threat from these types of behaviors, PayPal, in coordination with other industry partners, launched a program over a year ago called DMARC, which is meant to increase email trust and combat rampant email deception and fraud, such as spam and phishing. DMARC, which stands for Domain-based Message Authentication, Reporting & Conformance, builds on previous email authentication advancements, with strong protection of the author's address and creating a feedback loop from receivers back to legitimate email senders. DMARC standardizes how email receivers perform email authentication using the well-known Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) mechanisms. This means that senders will experience consistent authentication results for their messages at AOL, Gmail, Hotmail, Yahoo! and any other email receiver implementing DMARC. The program removes the guesswork from the receiver's handling of any failed messages, limiting or eliminating the user's exposure to potentially fraudulent and harmful messages. DMARC also provides a way for the email receiver to report back to the sender about messages that pass and/or fail DMARC evaluation.

In its first year, DMARC:

- Protected 60 percent of the world's email boxes or 1.976 billion of the estimated 3.3 billion email boxes worldwide. Protected 80 percent of US typical consumer mailboxes;
- Has been adopted by the world's largest consumer email providers– AOL, Comcast, Google, Mail.ru, Microsoft, NetEase, Xs4All, and Yahoo!;
- Can claim 50 percent of the top 20 sending domains publish a DMARC policy, with 70 percent of those domains asserting a policy that directs receivers to take action against unauthenticated messages; and

- Rejected hundreds of millions of potentially fraudulent messages. As an example, in November and December 2012, more than 325 million messages were rejected as purporting to be "From" domains with a DMARC reject policy.

Identity Management and Authentication

The Internet, especially with recent rapid mobile and cloud expansion, exposes users and enterprises, more than ever before, to fraud. We at PayPal believe it is critical to know who you're dealing with on the Internet at all times. Therefore, my team has also been very engaged in efforts to create a reliable identity management system to promote identity and stronger authentication. As a company that facilitates secure online and mobile financial transactions, it is critical that we have the ability to authoritatively authenticate our users. We strongly support efforts to create a workable "Identity Ecosystem" — where stakeholders work to protect individuals, businesses, and public agencies from the high costs of cyber crimes, like identity theft and fraud, while simultaneously helping to ensure that the Internet continues to support innovation and a thriving marketplace of products and ideas. To accomplish this goal, we have participated in two different programs, The National Strategy for Trusted Identities in Cyberspace (NSTIC) and The Fast Identity Online (FIDO) Alliance.

As many of you know, NSTIC is a White House initiative, led by the National Institute of Standards and Technology, which is intended to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of sensitive online transactions. The program has been mostly led by the private sector, in partnership with the federal government, consumer advocacy organizations, privacy experts, state and local agencies, and others. Organizations representing 18 different business and infrastructure sectors and 70 different nonprofit and federal advisory groups have participated in the development of the "Strategy".

NSTIC differs from past efforts to encourage trusted IDs in several ways. From the outset, the NSTIC has involved the private sector as a partner in the effort. For instance, members of my team have served as significant contributors to the Identity Ecosystem Steering Group (IDESG) and Brett McDowell of PayPal current chairs the IDESG Management Council.

In our work at the IDESG we've worked diligently to ensure that the rules and practices put in place do actually fulfill the promise of NSTIC.

We have consistently advocated that trustworthy online identity is a key component of a healthy Internet ecosystem. PayPal will be offering more services to our customers over the coming months that directly support the NSTIC vision, which we expect will result in many new benefits to both our customers and the Internet overall.

PayPal was also one of the co-founders of The Fast Identity Online (FIDO) Alliance. Formed in July 2012, with Lenovo, Nok Nok Labs, Infineon and others, the goal of the Alliance is to address the lack of interoperability among strong authentication devices as well as the problems users face with creating and remembering multiple usernames and passwords. The FIDO Alliance plans to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. This new standard for security devices and browser plugins will allow any website or cloud application to interface with a broad variety of existing and future FIDO-enabled devices that the user has for online security.

How it works is that our protocol-based model will automatically detect when a FIDO-enabled device is present, meaning that end users from the banking, corporate, public sector or consumer arenas could be given the option to replace passwords with authentication methods embedded in hardware. It can be deployed in biometric tools such as fingerprint scanners, voice and facial recognition technology, or more traditional security aids such as one-time password (OTP) tokens or trusted platform models.

The FIDO Alliance is a private sector and industry-driven collaboration to combat the very real challenge of confirming every user's identity online. By giving users choice in the way they authenticate and taking an open-based approach to standards, we can make universal online authentication a reality. We wanted to provide an easier and safer solution to every company, vendor, and organization that needs to verify user identity.

The National Cyber Security Alliance and Promoting Education Awareness

As a responsible corporate citizen, we believe that we have an important role to play in education and awareness campaigns that help consumers and businesses protect themselves online. Currently, PayPal is on the board of the National Cyber Security Alliance (NCSA) and we are very engaged in their Stay Safe Online national program. We believe in the NCSA's mission which is to "educate and empower a digital society to use the Internet safely and securely at home, work, and school, while protecting the technology, individuals' use, the networks they connect to, and our shared digital assets".

In cooperation with a number of large Internet companies and major web browser makers, PayPal participated in an education campaign in 2010 to encourage our customers to upgrade their web browser to the latest and most secure version.

Recommendations for Federal Policymakers

Although it is the responsibility of industry leaders, like PayPal, to ensure the safety and security of our platforms and our users, federal policymakers have an important role to play in creating a secure Internet and mobile ecosystem. Here are some of our recommendations for areas where the federal government, and specifically Congress, can lend a helping hand.

Research and Reliable Data

As you know, the Internet offers tremendous benefits and efficiencies to businesses and consumers and over the years this has led to a burgeoning Internet-enabled industry. However, as online business transactions increase and more and more consumers adopt Internet and mobile services, cyber criminals are given greater access to business assets and personal information than ever before, opening up risks for intellectual property theft, identity theft, and other crimes.

What we have found from our years of combatting cybercrime, is quantifying the full cost is difficult if not impossible because many incidents are not reported. Estimates of the

magnitude and scope of cybercrime vary widely, making it difficult for policymakers and industry to fully understand the severity of the problem and the level of effort that will be needed to combat it. However, based on recent studies, cybercrime is definitely a growing problem. For instance, a 2011 government-sponsored study in the United Kingdom found that cybercrime cost £27 billion (about $44 billion) in the UK alone, with businesses bearing three-quarters of that cost. The Federal Bureau of Investigation's Crime Complaint Center (IC3) received 22% more self-reported cybercrime complaints in 2009 than the previous year — and that the dollar value of these incidents was skyrocketing, up 111% in 2009 to more than $550 million. It's clear that business is currently sustaining significant losses to cybercrime, but until we know how much money is being lost, where the money is going and whether or not the responsible parties can be held accountable, it will be hard to create a framework that really addresses the problems.

It is our recommendation that policymakers sponsor research that helps to fill in some of the information gaps that currently exist as it relates to cybercrime. We believe that this research will be a critical tool in arming policymakers, law enforcement and industry against the growing threat of cybercrime.

Increased Resources for Law Enforcement and Greater Workforce Development

The difference between the effectiveness of law enforcement in the physical world and on the Internet could not be more striking. In the real world even minor crimes such as vandalism and burglary resulting in relatively low dollar losses merit at least a visit by a police officer, while online crimes exceeding $25,000 frequently go uninvestigated, much less prosecuted. We believe that this unfortunate reality is mainly due to insufficient funding for cybercrime law enforcement and a general lack of trained cyber experts within law enforcement and policy circles.

We believe that there is a significant increase or a reprioritization needed in the funding of agencies which investigate and prosecute cybercrime offenses. We don't offer a specific proposal for the appropriate funding levels but we believe the case for additional resources will be easily made once better data is available regarding the scope of the problem. We recommend

that policymakers look to find ways to help law enforcement agencies address these resource needs.

In addition, we encourage policy makers to find ways to encourage greater workforce development and training for cybersecurity professionals. Most important for PayPal and eBay is training for computer programmers in secure development practices. While computer science programs have been quite effective in turning out students with the appropriate general programming knowledge and skills necessary for today's jobs, they have not kept up with the demand of security conscious companies who need programmers who know how to develop applications securely and free from technical flaws. While we are seeing progress at a number of institutions we believe substantial investment is warranted in this field.

Increase Enforcement Across Borders

The European convention on cybercrime has represented an extremely important framework for dealing with cybercrime internationally. However, there are two ways in which it has fallen short.

The convention allows nations to cooperate with each other in investigating cases of cybercrime. It permits one state to request that a second state preserves and supplies the necessary data needed to support a particular investigation. However, the mechanisms used to request the data are antediluvian: Multi-Lateral Assistance Treaties (MLATs), and "Letters Rogatory". In all of the cases where we have worked with multi-country investigations, we have never witnessed a case in which the data has been returned to the requesting law enforcement agency in under three months. We have found that six months is more common, and we have heard of cases where the data has been returned more than two years after it was originally requested. Given the speed at which cyber attacks move, this slow response time effectively hobbles the investigating law enforcement agency and frequently cripples investigations. During this time, the criminals are allowed to keep victimizing citizens and law abiding organizations.

We agree that there needs to be some level of supervision, and approval, such that rogue officers (or worse) cannot request arbitrary information from another state, without good purpose. But, in the age of the Internet, most workflow functions can be highly automated. The technology to do this exists, and is readily available. We recommend that policymakers consult our domestic law enforcement organizations who best understand how to fix current practices and make cross border enforcement a more coordinated and streamlined process.

Removing Barriers to Private and Public/Private Cooperation

In our testimony we have highlighted a number of cases where we have partnered with private and public entities to find solutions to the growing threat of cybercriminal activities. Although we have been very successful in some of these cases, we believe that we could accomplish more by working with policymakers to remove some of the barriers that prevent private industry from working together to protect the Internet ecosystem.

One of those barriers relates to information sharing between private companies. We understand and strongly support the need of strong privacy protections for consumers and individual businesses, however, we also believe that outdated provisions of certain laws, such as the Electronic Communication Privacy Act of 1986 (ECPA), have been interpreted in a way that impedes the ability of private industry to work together to combat cybercrime in a way that protects ourselves and our users.

For instance, as I testified, our DMARC program has been very successful in stopping unauthenticated emails from reaching inboxes. However, the DMARC program is not necessarily as effective as it could be because of the limitations the current statute places on private-to-private information sharing, even in cases of security. Not only does DMARC provide a way for email providers to tell whether or not an email is authentic, but it also provides a way for the email receiver to report back to the sender about messages that pass and/or fail DMARC evaluation. This reporting is a matter of common sense. If cybercriminal is using a company's trademark and brand in an unauthorized manner, we believe that company would want to know, and should know, where that email is coming from in a timely manner so that they

can work with the proper authorities to take down the rogue website. Unfortunately, some current interpretations of ECPA prohibit voluntary information sharing of this nature between private companies. Unfortunately, instead of helping to protect companies and consumers from bad actors like its original intent, these privacy laws are serving to immunize illegal actions from further scrutiny. We ask that policymakers review ECPA and other potentially outdated laws that can prohibit companies from meaningfully protecting the security and privacy rights of their users and themselves.

Increase Consumer Education Awareness

It is clear from a variety of sources, that most consumers have little idea how to protect themselves online. However, it is also clear that the problem is much larger than the scope of work happening today. There are many studies that show the majority of Internet users are both afraid of the risk of using the Internet, and simultaneously don't have the information needed to protect themselves online.

While the education efforts from organizations like NCSA are helpful, they are simply not at the scale needed to help hundreds of millions of Internet users across the United States. This area needs to experience significant increase in investment from both private industry and government stakeholders.

In addition, we believe that there should be some consideration of introducing cyber-safety education curriculum into public schools. There are a number of studies showing how these "digital natives" are in fact more trusting of the Internet. Although it is important that we continue to foster adoption of Internet and mobile technologies at a young age, we also think it is necessary to educate children on the potential risks and dangers and how to avoid them. This problem is more tractable than general consumer outreach, as there are formal channels—i.e. schools—by which this group of users can be reached. All that is needed is the development of a formal safety and security curriculum, and an insistence that this topic becomes one of the core areas taught to students.

Establish a Coordinated Internet Safety Framework

When we look at other forms of technical innovation throughout history, we can clearly see that these innovations were coupled with attendant public policy, self-regulation and public reaction that were instructive for understanding the various roles and responsibilities that each stakeholder had to play in order to maintain the safety and benefits of the technology. For instance, today, when you ask an individual the parties responsible for ensuring the safety on our highways, most people would probably be able to instinctively respond with the names of a few of the responsible stakeholders, such as motorists, local and state law enforcement, state and federal departments of transportation, and the National Highway Traffic Safety Administration. Most Americans know this because there is a solid framework that was created and implemented years ago that is intended to keep motorists safe while traveling on our nation's highway system.

However, when you ask that same question, but replace highways with the Internet, the same individual would most likely fail to give a response. Unfortunately, we as a country have failed to adopt a framework for the Internet and mobile ecosystem that clearly lays out the various stakeholders and jurisdictions involved and the roles that each stakeholder has to ensure users safety while they are traveling on the World Wide Web.

We recommend that Congress work with various stakeholders, including consumers, industry, policymakers, regulators, academics, and civil liberty groups, to create a national framework that creates a clear and concise model for how our nation keeps one of our greatest engines of economic growth safe and secure for all users.

The Cybersecurity Enhancement Act

In light of these policy recommendations, I did want to take a few minutes to praise the work that the House Science, Space & Technology Committee has done to address some of the cybersecurity challenges facing our nation. PayPal appreciates the bipartisan efforts of the Committee over the past few years to create a legislative framework that creates some innovative

solutions to issues such as cybersecurity R&D, education and workforce training, and standards development. Importantly, it achieves these ends without creating undesired side-effects.

In particular, we are very appreciative and supportive of the following provisions within the legislation and would welcome the opportunity to work with Members of the Committee on these priorities:

- Section 104 – Social and behavioral research in cybersecurity: This section is well aligned with a number of our efforts and our recommendations in terms of areas that need additional research. In particular, we think that Human Computer Interaction (HCI) topics in security are a new frontier and we applaud the Committee for their consideration of these issues.

- Section 109 – Security automation and Checklists: Improved automation and repeatability are key. We appreciate the Committee's attention to these issues and believe that this work will have a positive impact.

- Section 205 – Strengthen Authentication for Identity Systems: As I testified, this is the wave of the future in terms of improving security of the Internet and mobile ecosystems and this is completely aligned with our work on FIDO and NSTIC.

Conclusion

To conclude, PayPal is committed to providing our customers with the safety and security that they not only deserve, but expect. We recognize that security is a key component of their experience and the trust they place with us. As technology changes, as the world changes, the security measures that we adopt will continue to change. However, my role is to keep up with these rapidly evolving trends and not only surpass the bar that our consumers and employees challenge us to reach on a daily basis, but work to find solutions that will benefit not just PayPal but the entire Internet and mobile ecosystem. It is our hope that in the years to come the challenges we face from cybercrime will be a faint memory. But until then, PayPal is committed

to partnering with policymakers and private and public stakeholders to ensure that we do everything in our power to create an ecosystem that is safe and secure.

I appreciate the opportunity to testify before the Committee, and I look forward to your questions.