SONY
COMPUTER ENTERTAINMENT®

Sony Computer Entertainment America
919 East Hillsdale Blvd.
Foster City, California 94404-2175
650 655 8000
650 655 8001 Fax

May 3, 2011

The Honorable Mary Bono Mack
Chairman
Subcommittee on Commerce, Manufacturing, and Trade
United States Congress
2125 Rayburn House Office Building
Washington, D.C. 20515

The Honorable G. K. Butterfield
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
United States Congress
2125 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Bono Mack and Ranking Member Butterfield:

Thank you for giving me this opportunity to respond to questions from the House Energy and Commerce Committee, Subcommittee on Commerce, Manufacturing and Trade.

Sony now faces a large-scale cyber-attack involving the theft of personal information. This cyber-attack came shortly after Sony Computer Entertainment America was the subject of denial of service attacks launched against several Sony companies and threats made against both Sony and its executives in retaliation for enforcing intellectual property rights in U.S. Federal Court. We are currently dealing with all aspects of this cyber-attack and have our personnel deployed and working around the clock to get the systems back up and to make sure all our customers are informed of the data breach and our responses to it. We expect to restore most services to our customers shortly. We have received so far no confirmed reports of illegal usage of the stolen information.

In dealing with this cyber-attack, the company has operated on the basis of several key principles:

1. Act with care and caution. This is why Sony Network Entertainment America Inc. ("Sony Network Entertainment America"), which operates the PlayStation Network and Qriocity services (collectively, "PlayStation Network"), has taken the almost unprecedented step of shutting down the affected systems as soon as threats were detected and is keeping them down, even at substantial cost to the company, until all changes to strengthen security are completed. We have tried to err on the side of safety and security in making these decisions and judgments.

2. Provide relevant information to the public when it has been verified. Sony Network Entertainment America immediately hired a highly regarded information technology security firm and supplemented that firm with additional expertise and resources over several days. Sony Network Entertainment America then released information to its consumers when we and those experts believed that information was sufficiently confirmed. The truth is that retracing the steps of experienced cyber-

attackers is a highly complex process that takes time to carry out effectively. At the same time that the experienced attackers were carrying out their attack, they also attempted to destroy the evidence that would reveal their steps.

3. Take responsibility for our obligations to our customers. We have apologized for the inconvenience caused by the illegal intrusion into our systems and offered a free month of service in addition to the number of days the systems are down as part of a "Welcome Back" program for our customers. We are also offering our customers in the U.S. complimentary identity theft protection services.

4. Work with law enforcement authorities to assist in the apprehension of those responsible and cooperate with all authorities on meeting our regulatory requirements. One of our first calls was to the FBI, and this is an active, on-going investigation.

I am of course aware of the criticism Sony has received for the time taken to disclose information to our customers. I hope you can appreciate the extraordinary nature of the events the company was facing - brought on by a criminal hacker whose activity was neither immediately nor easily ascertainable. I believe that after you review all the facts you will agree that the company has been acting in good faith to release reliable information in accordance with its legal and ethical responsibilities to its valued customers.

We have been investigating this intrusion around the clock since we discovered it, and that investigation continues today. Just this past Sunday, May 1st, we learned that a likely theft from another Sony company's online service had previously gone undetected, even after highly trained technical teams had examined the network infrastructure that had been attacked around the same time as the PlayStation Network. What is becoming more and more evident is that Sony has been the victim of a very carefully planned, very professional, highly sophisticated criminal cyber attack designed to steal personal and credit card information for illegal purposes. Sunday's discovery that data had been stolen from Sony Online Entertainment only highlights this point.

When Sony Online Entertainment discovered this past Sunday afternoon that data from its servers had been stolen, it also discovered that the intruders had planted a file on one of those servers named "Anonymous" with the words "We are Legion." Just weeks before, several Sony companies had been the target of a large-scale, coordinated denial of service attack by the group called Anonymous. The attacks were coordinated against Sony as a protest against Sony for exercising its rights in a civil action in the United States District Court in San Francisco against a hacker.

While protecting individuals' personal data is the highest priority, ensuring that the Internet can be made secure for commerce is also essential. Worldwide, countries and businesses will have to come together to ensure the safety of commerce over the Internet and also find ways to combat cybercrime and cyber terrorism.

Almost two weeks ago, one or more cyber criminals gained access to PlayStation Network servers at or around the same time that these servers were experiencing denial of service attacks. The Sony Network Entertainment America team did not immediately detect the criminal intrusion for several possible reasons. First, detection was difficult because of the sheer sophistication of the intrusion. Second, detection was difficult because the criminal hackers exploited a system software vulnerability. Finally, our security teams were working very hard to defend against denial of service attacks, and that may have made it more difficult to detect this intrusion quickly – all perhaps by design.

Whether those who participated in the denial of services attacks were conspirators or whether they were simply duped into providing cover for a very clever thief, we may never know. In any case, those who participated in the denial of service attacks should understand that - whether they knew it or not - they were aiding in a well planned, well executed, large-scale theft that left not only Sony a victim, but also Sony's many customers around the world.

Making the Internet safe for entertainment, commerce and education is a paramount government interest. The criminal cyber-attacks on Sony have been and will continue to be perpetrated on other companies as well. If not addressed, these types of attacks could become commonplace. Creating more stringent guidelines for maintaining and policing storage of personal information may be necessary in our current climate, but, make no mistake, without addressing the need for strong criminal laws and sanctions and, most importantly, enforcement of these laws, there will not be any meaningful security on the Internet.

Sony is grateful for the assistance it has received from law enforcement and appreciates this opportunity to raise these issues with this Committee as it considers how to build an environment where social networks and commerce on the Internet can develop uninhibited by security risks.

Turning to Sony's responses to the Committee's questions:

1. When did you become aware of the illegal and unauthorized intrusion?

On April 19, 2011 at 4:15 p.m. PDT, members of the Sony Network Entertainment America network team detected unauthorized activity in the network system, specifically, that certain systems were re-booting when they were not scheduled to do so. The network service team immediately began to evaluate this activity by reviewing running logs and analyzing information in order to determine if there was a problem with the system.

On April 20, 2011, in the early afternoon, the Sony Network Entertainment America team discovered evidence that indicated an unauthorized intrusion had occurred and that data of some kind had been transferred off the PlayStation Network servers without authorization. At the time, the network service team was unable to determine what type of data had been transferred, and they therefore shut the PlayStation Network system down.

2. How did you become aware of the breach?

Sony Network Entertainment America became aware of the PlayStation Network intrusion as described above. The Sony Network Entertainment America team became aware of a transfer of data out of the system also as described above. Sony Network Entertainment America then began the exhaustive and highly sophisticated process of identifying the means of access and the nature and scope of the theft. That investigation is on-going to this day.

3. When did you notify the appropriate authorities of the breach?

On April 22, 2011, Sony Computer Entertainment America's general counsel provided the FBI with information about the intrusion. (Sony Computer Entertainment America oversees the PlayStation brand in North America and has been involved with the PlayStation Network's operation since its inception). The forensic experts that Sony Network Entertainment America had retained had not determined the scope or effect of the intrusion at the time the FBI was contacted. A meeting was set up to provide details to law enforcement for Wednesday April 27, 2011.

Following an extensive investigation by a team of external forensic computer experts with the assistance of the internal network service team, Sony Network Entertainment America and Sony Computer Entertainment America coordinated to provide public notice of the intrusion on April 26, 2011. On the same day, Sony Network Entertainment America notified the applicable regulatory authorities in the states of New Jersey, Maryland, and New Hampshire. On April 27, 2011, Sony Network Entertainment America also notified regulatory authorities in the states of Hawaii, Louisiana, Maine, Massachusetts, Missouri, New York, North Carolina, South Carolina, Virginia and Puerto Rico of the criminal intrusion described above.

4. Why did you wait to notify your customers of the breach?

The PlayStation Network is a complex network, consisting of approximately 130 servers, 50 software programs and 77 million registered accounts. The basic facts of what occurred after the intrusion bear this out.

On April 19, 2011, the Sony Network Entertainment America network team discovered that several PlayStation Network servers unexpectedly rebooted themselves and that unplanned and unusual activity was taking place on the network. This activity triggered an investigation. The network team took four servers off line and an internal assessment began. The internal assessment of these four servers continued through the end of the business day and into the evening. The next day, April 20th, Sony Network Entertainment America mobilized a larger internal team to assist the investigation of the four suspect servers. This internal team discovered the first credible indications that an intruder had been in the PlayStation Network systems, and six more servers were identified as possibly being compromised. Sony Network Entertainment America immediately decided to shut down all of the PlayStation Network services.

In the afternoon of April 20th, Sony Network Entertainment America retained a recognized security and forensic consulting firm to mirror the servers to enable forensic analysis to begin. The type of mirroring required to provide meaningful information in this type of situation had to be meticulous. Many hours were needed simply to mirror servers before analysis could begin. Sony Network Entertainment America and its outside forensics team began to work on mirroring the servers.

The scope and complexity of the investigation grew substantially as additional evidence about the attack developed. On April 21, 2011, Sony retained a second recognized computer security and forensic consulting firm to assist in the investigation, to provide more manpower to image the servers and to conduct a forensic analysis of all aspects of the suspected security breach.

The team took until the afternoon of April 22, 2011 to complete the mirroring of nine of the 10 servers that were suspected of being compromised. By the evening of April 23, 2011, the forensic teams were able to confirm that intruders had used very sophisticated and aggressive techniques to obtain unauthorized access, hide their presence from system administrators, and escalate privileges inside the servers. Among other things, the intruders deleted log files in order to hide the extent of their work and activity within the network. Now Sony Network Entertainment America knew it was dealing with a sophisticated hacker and (on Easter Sunday) decided that it needed to retain yet another forensic team with highly specialized skills to assist with the investigation. Specifically, this firm was retained to provide even more manpower for forensic analysis in all aspects of the suspected security breach, and, in particular, to use their special skills to determine the scope of the data theft. By April 25, 2011, the forensic teams were able to confirm the scope of the personal data that they believed had been taken but could not rule out whether credit card information had been accessed.

Sony Network Entertainment America was of course aware of its affirmative obligations under various state statutes to conduct a reasonable and prompt investigation to determine the scope of breach and depth of the breach and to restore the integrity of our network system. Sony Network Entertainment America further understood its obligation to report its finding to consumers if certain, specific kinds of personal information could have been compromised. As this Committee knows, there are a variety of state statutes that apply and several that have conflicting or inconsistent requirements, but given the global nature of the network, Sony Network Entertainment America needed to be mindful of them all. Throughout the process, Sony Network Entertainment America was very concerned that announcing partial or tentative information to consumers could cause confusion and lead them to take unnecessary actions if the information was not fully corroborated by forensic evidence. For example, as of April 25, 2011, Sony had not and could not determine if credit card information had been accessed and, while no evidence existed at the time that this type of information had been taken, we ultimately could not rule out that possibility entirely based on the reports of the forensics teams. Given that situation, on April 26, 2011, Sony Network Entertainment America and Sony Computer Entertainment America notified consumers that their personal information had been taken and that the companies could not rule out the possibility that credit card data had been stolen as well.

5. Was the information obtained applicable to all accounts or a portion of the accounts? How many consumers or accounts were impacted by this breach, and how did you ascertain the number?

Information appears to have been stolen from all PlayStation Network user accounts, although not every piece of information in those accounts appears to have been stolen. The criminal intruders stole personal information from all of the approximately 77 million PlayStation Network and Qriocity service accounts.

6. Have you identified how the breach occurred?

Yes, we believe so. Sony Network Entertainment America is continuing its investigation into this criminal intrusion, and more detailed information could be discovered during this process. We are reluctant to make full details publicly available because the information is the subject of an on-going criminal investigation and also the information could be used to exploit vulnerabilities in systems other than Sony's that have similar architecture to the PlayStation Network.

7. Have you identified the individual(s) responsible for the breach?

No.

8. What information was obtained by the unauthorized individual(s) as a result of this breach, and how did you ascertain this information?

Based on the activity of the intruder, we know that queries were made in the PlayStation Network system database for user account information related to name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PlayStation Network online ID.

As of today, the major credit card companies have not reported that they have seen any increase in the number of fraudulent credit card transactions as a result of the attack, and they have not reported to us any fraudulent transactions that they believe are a direct result of the intrusions described above.

9. How many PlayStation Network account holders provided credit card information to Sony Computer Entertainment?

Globally, approximately 12.3 million account holders had credit card information on file on the PlayStation Network system. In the United States, approximately 5.6 million account holders had credit card information on file on the system. These numbers include active and expired credit cards.

10. Your statement indicated you have no evidence at this time that credit card information was obtained, yet you cannot rule out this possibility. Please explain why you do not believe credit card information was obtained and why you cannot determine if the data was in fact taken.

As stated above, Sony Network Entertainment America has not been able to conclude with certainty through the forensic analysis done to date that credit card information was not transferred from the PlayStation Network system. We know that for other personal information contained in the account database, the hacker made queries to the database, and the external forensics teams have seen large amounts of data transferred in response to those queries. Our forensics teams have not seen queries and corresponding data transfers of the credit card information.

11. What steps have you taken or do you plan to take to prevent future such breaches.

The new security measures being implemented include the following:

- Added automated software monitoring and configuration management to help defend against new attacks;
- Enhanced levels of data protection and encryption;
- Enhanced ability to detect software intrusions within the network, unauthorized access and unusual activity patterns;
- Implementation of additional firewalls; and
- The company also expedited a planned move of the system to a new data center in a different location with enhanced security.
- The naming of new Chief Information Security Officer (CISO) directly reporting to the Chief Information Officer, Sony Corporation.
-

12. Do you currently have a policy that addresses data security and retention practices? If not, why not? If so, what are those practices and do you plan any changes in your policies as a result of this breach?

Yes, we do have policies that address data security and retention practices.

Sony utilizes a global framework for providing policies to its group companies based on the international information security standard called "ISO/IEC 27001" to ensure consistent standard information security practices for each operating company. The Global Information Security Policy ("GISP") sets forth the company's information security management structure and administrative, technical and physical safeguards to protect the confidentiality, integrity, and availability of non-public information. The GISP also defines the overall direction and policy of Sony Group's information security program and the authorities and responsibilities for information security management. Additionally, Sony provides a set

of 14 standards, Global Information Security Standards ("GISS"), that specify the types of controls needed for the different categories of information security management (e.g., information classification, access controls and HR security).

Continued application of these policies and practices, in addition to, an expedited move to our new enhanced security data facility, are the changes being made as a result of this breach.

13. What steps have you taken or do you plan to take to mitigate the effects of this breach? Do you plan to offer any credit monitoring or other services to consumers who suffer actual harm as a result of this breach?

Sony Network Entertainment America is committed to helping its customers protect their personal data and will offer its U.S. account holders complimentary identity theft protection services. Because the breach affects customers worldwide, different programs may be offered in other territories.

Sony Network Entertainment America is also creating a "Welcome Back" program to be offered worldwide, which will be tailored to specific markets to provide our consumers with a selection of service options and premium content as an expression of the company's appreciation for their patience and support.

Central components of the "Welcome Back" program will include:

- Each territory will be offering selected PlayStation entertainment content for free download. Specific details of this content will be announced in each region soon.
- All consumers coming back to the PlayStation Network will be provided with 30 days of free membership in the PlayStation Plus premium subscription service. Current PlayStation Plus subscribers will have their subscriptions extended for the number of days PlayStation Network and Qriocity services were unavailable and, in addition, will receive 30 days of free service.
- Music Unlimited subscribers (in countries where the service is available) will have their subscriptions extended for the number of days PlayStation Network and Qriocity services were unavailable and, in addition, receive 30 days of free service.

* * * *

I want to thank this Committee for giving me this opportunity to respond to its questions. I hope I have been able to convey the extraordinary circumstances and challenges that have confronted the employees of Sony Network Entertainment America and Sony Computer Entertainment America over the past few days and weeks. My employees were facing and have endured an unprecedented large-scale criminal cyber-attack. They were faced with very difficult decisions and often-times conflicting concerns and objectives. Throughout this challenging period, they acted carefully and cautiously and strove to provide correct and accurate information while balancing concerns for our consumers' privacy and need for information.

This Committee is rightfully concerned to protect the information and privacy of individuals on the Internet and to ensure that companies have robust security and protection practices. We ask the Committee to consider as well the connection between data security and the cybercrimes and cyber terrorism that threaten to make the Internet unsafe for consumers and commerce. We very much appreciate the Committee's efforts to put in place laws to protect us from these very real threats.

Respectfully submitted,

RRR for Kazuo Hirai

Kazuo Hirai
Chairman of the Board of Directors
Sony Computer Entertainment America LLC

cc: The Honorable Fred Upton
Chairman
U.S. House of Representatives
Committee on Energy and Commerce

The Honorable Henry A. Waxman
Ranking Member
U.S. House of Representatives
Committee on Energy and Commerce