Wells Fargo Insurance Services USA, Inc.

WELLS FARGO INSURANCE

Privacy and Network Security Liability in Higher Education

Tri-State Association of Financial Aid Administrators - Annual Meeting

David Shannon, Marshall, Dennehey, Warner, Coleman & Goggin

John Farley, Wells Fargo Insurance Services

Ocean City, MD
November 6, 2012

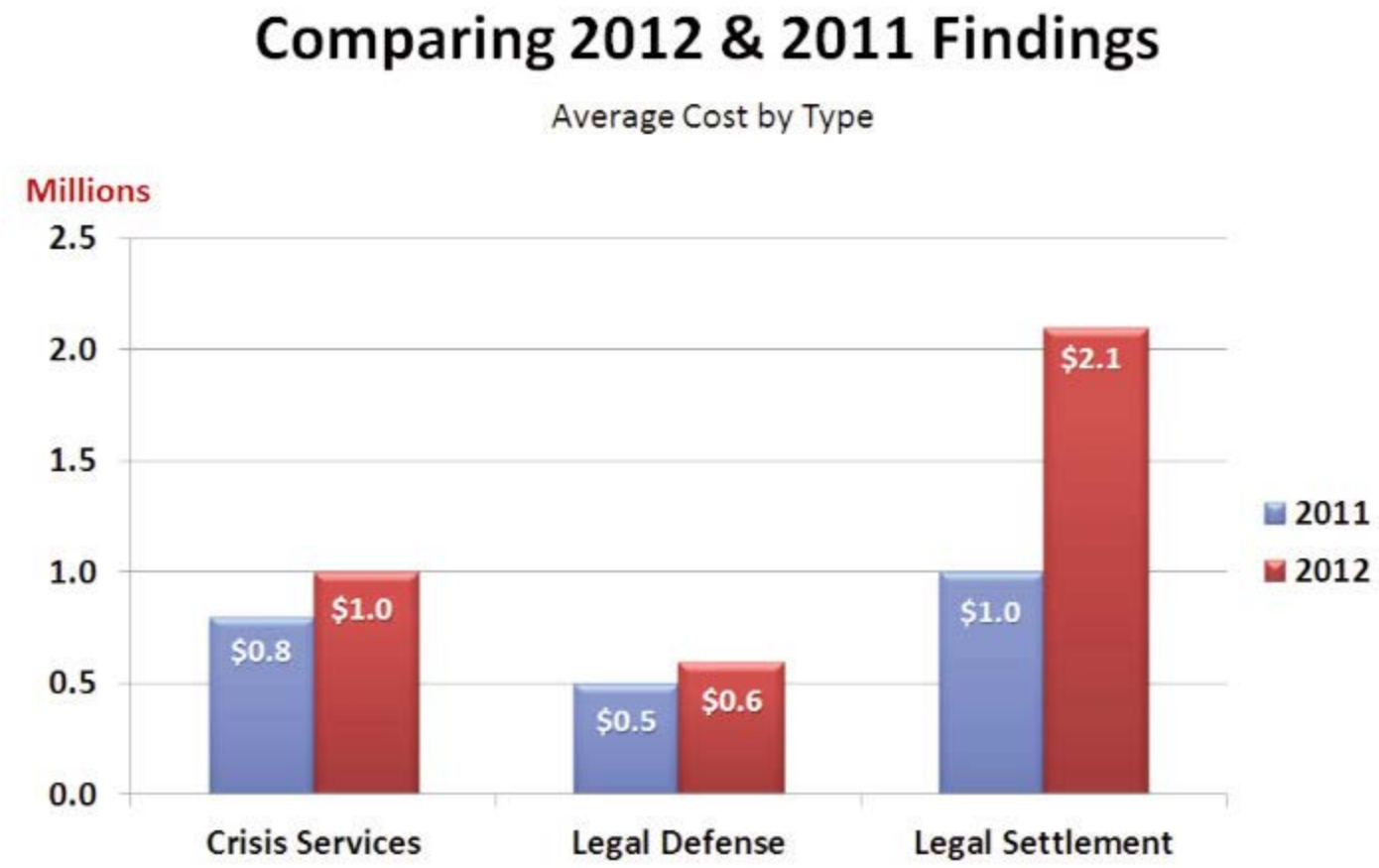
Agenda

- Recent data breach studies
- Causes of data breaches
- High risk industries
- What is at risk for higher education
- Legal and financial consequences
- Recent higher education breaches
- Data breach best practices
- Vendor management
- Insurance coverage
- State laws
- Federal laws

Ponemon Institute 2011 cost of data breach study

- Analyzed 49 breaches in 14 business sectors
- Average cost per record was $194
- Cost decreased when an organization had a CISO or used outside consultants after a breach
- Cost increased when the breach was caused by a third party, involved a lost or stolen device, or notification went out without a thorough assessment of the breach

Cyber Liability & Data Breach Insurance Claims Study - NetDilligence® 2012



The legal and financial consequences

- Crisis management
- Legal liability
- Business interruption costs
- Fines

Causes of security breaches

- Disposal of documents and computers
- Hacking – external and internal
- Phishing and other social engineering tools
- Lost or missing or stolen laptops, external hard drives, thumb drives
- Internet - web portal like Blackboard

High hazard industry classes

- Schools, colleges, and universities
- Healthcare
- Financial institutions
- Retail
- eCommerce companies
- Information and data services companies
- Credit card processors
- Public entities

Why is higher education at risk?

- Databases are decentralized
- Access to information is encouraged
- Higher education has large amounts of sensitive information including research, intellectual property, and government secrets
- Population is prone to questioning the institution's handling of data security events and/or testing the security of the institution

What is at risk?

- Personally Identifiable Information (PII)
  - Social security numbers
  - Driver's license information
  - Credit cards, debit cards, and other payment information
  - Financial information, like account balances, loan history, and credit reports
  - Non-personally identifiable Information, like email addresses, phone lists, and home address that may not be independently sensitive, but may be more sensitive with one or more of the above
- Education records
  - Any record, maintained by an institution or agent of the institution, where a student can be personally identified (for example, transcripts or other records obtained from a school in which a student was previously enrolled)
- Employee information
  - Employers have at least some of the above personal information on all employees
- Business partners information
  - Vendors and business associates may provide some of the above information

Recent cases

Ohio State University - December 2010

A hacker accessed a server that stored the names, social security numbers, dates of birth and addresses of 760,000 current and former faculty, students, applicants, and others affiliated with the university.

It is estimated that it could cost the university $4 million.

Recent cases, continued

University of Nebraska – May 2012

A hack into the electronic database breached access to the personal records of 640,000 applicants, students, alumni dating back to 1985, and applicants at all four university campuses.

Recent cases, continued

University of Hawaii - 2009 through 2011

5 data breach events. A faculty member inadvertently uploaded files containing the information to an unprotected server, exposing the names, academic performance, disabilities, and other information of more than 100,000 students, alumni, faculty and staff. The data was posted online for one year.

A class action lawsuit was settled. It was the largest class action settlement ever in the state of Hawaii.

Recent cases, continued

Yale University – August 2011

Yale accidently allowed a Google search engine to index a database containing private information about 43,000 former faculty, staff, and students. Yale administrators are blaming a change made in Google's software for the exposure.

The data had been public for 10 months from September 2010 to July 2011.

Data breach claim mitigation

- Assemble the response team before a breach occurs
- Deploy IT forensics
- Contact appropriate law enforcement
- Seek legal counsel – privacy attorney
- Conduct an incident risk assessment to:
  - Provide to regulators
  - Determine further notification requirements mandated by state and federal breach notice laws
- Utilize credit monitoring firms, call centers, and public relations firms, as needed
- Notify any relevant insurance carriers: Network Security & Privacy, Property, General Liability, K&R, Crime and/or Error & Omissions policies

What should you be asking?

- Have we analyzed our cyber liabilities?
- What legal rules apply to the information we maintain or kept by vendors, partners and other third parties? The laws surrounding breaches are complex.
- Have we assessed our legal exposure to governmental investigations?
- Have we assessed our exposure to suits by our customers, vendors or suppliers?
- Have we protected our organization in contracts with vendors?
- What laws apply in different states and countries in which we conduct business?
- Do we have adequate staffing to reasonably maintain and safeguard our important assets and processes?
- Have we prepared an incident response plan and business continuity plan?
- Do we have a documented, proactive crisis communications plan?

It is critical to have a solid incident response plan in place prior to any security or privacy breach.

It is critical to have a solid incident response plan in place prior to any security or privacy breach.

Due diligence on vendors is key.
Secondary is insurance requirements.

Vendor management and requirements

Due diligence on vendors is key.

Secondary is insurance requirements.

- IT and software Companies
  - Request Tech E&O to include network security and privacy coverage
  - Some Tech E&O policies have security and privacy exclusions
- Other business services – payroll, auditors
  - Request appropriate E&O coverage to include network security and privacy
- Credit card processors and acquiring banks
  - Request Network Security and Privacy coverage
- Other vendors that interact with your systems or sensitive information, or handle information on your behalf
  - Request Network Security and Privacy coverage

What can be covered under a network security and privacy policy?

- **Breach of Security:** Your liability to third parties arising out of a failure of your network security that results in a computer attack. Such failure can be caused by unauthorized access or use, transmission of a computer virus or a denial of service attack.
- **Invasion of Privacy:** Your liability arising from disclosure and release of confidential or personally identifiable information stored on your computer system caused by a failure of your network security.
- **Enterprise Privacy:** Your liability arising from any breach of privacy including violations of HIPAA, GLB or any state, federal or foreign privacy protection law (including regulatory defense expenses, notification expenses, credit monitoring, crisis management expenses)
- **Identity Theft:** Your liability arising from theft of personal information of your employees, customers or clients.

What can be covered under a network security and privacy policy?

- **Cyber Extortion:** Protection against threats or demands made against you involving your computer network.
- **Internet Media:** Defamation, Libel and Slander/Personal Injury – Liability arising out of the content disseminated on your Internet site; includes intellectual property infringement exposures
- **Business Interruption:** Business Interruption losses sustained by you arising from the interruption or suspension of your computer network, due to failure of security (including extra expenses)
- **Data Asset Coverage:** Information asset protection for you for property losses involving data, computer systems and information assets arising from a computer attack.

Network security and privacy GAP analysis

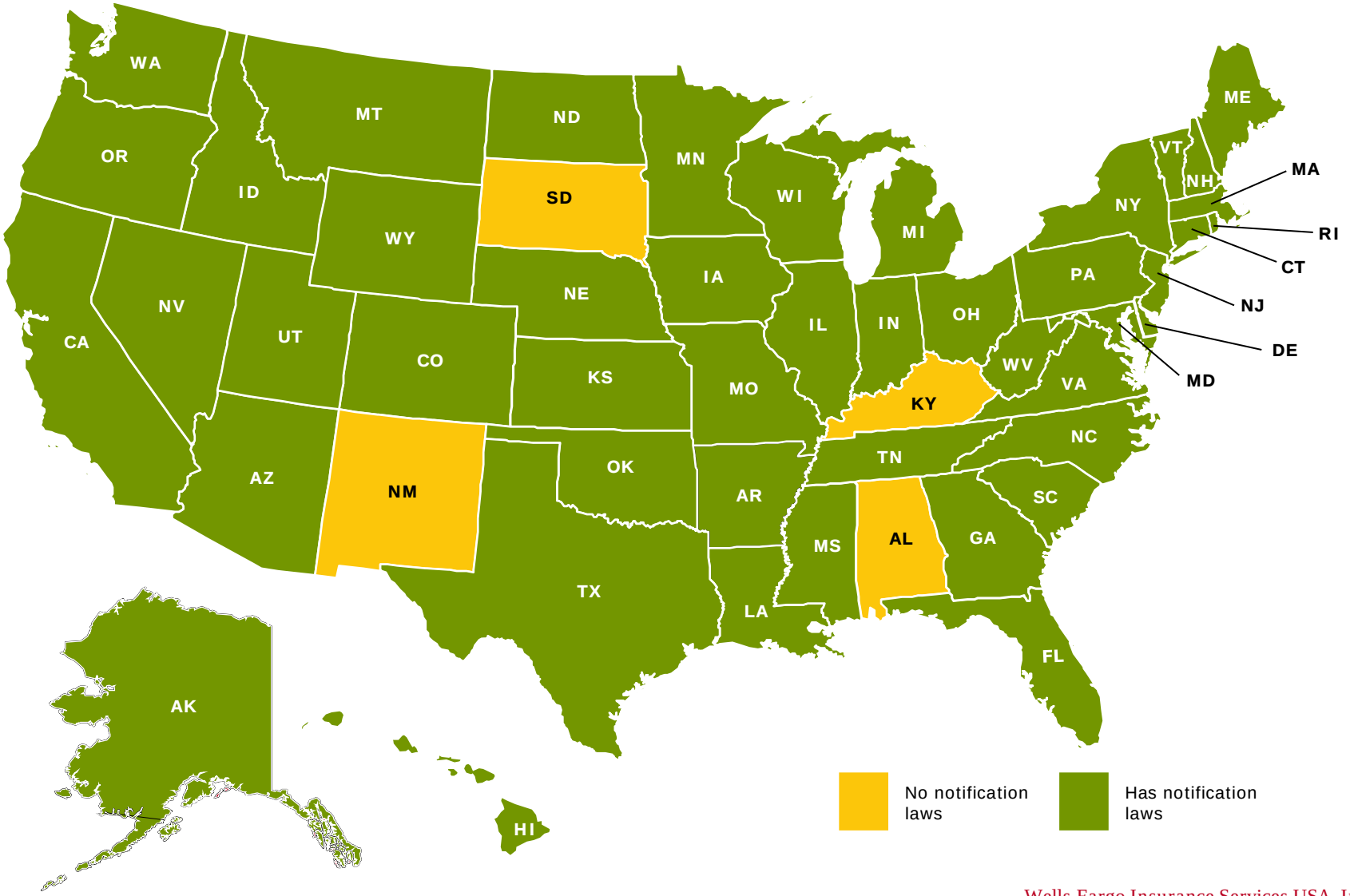
	Property	General Liability	Crime	K&R	E&O	Network Security & Privacy
1st Party Privacy and Network Risks						
Physical damage to data only	☐	☒	☐	☒	☐	☐
Virus/hacker damage to data only	☐	☒	☒	☒	☐	☑
Denial of Service (DOS) Attack	☐	☒	☒	☒	☐	☑
Business interruption loss from security event	☐	☒	☒	☒	☒	☑
Extortion or threat	☒	☒	☒	☑	☒	☑
Employee sabotage of data only	☒	☒	☐	☒	☐	☑
3rd Party Privacy and Network Risks						
Theft/disclosure of private information	☒	☐	☒	☒	☐	☑
Confidential corporate information breach	☒	☐	☒	☒	☐	☑
Technology E&O	☒	☒	☒	☒	☑	☒
Media liability (electronic content)	☒	☐	☒	☒	☐	☐
Privacy breach expense and notification	☒	☒	☒	☒	☒	☐
Damage to 3rd party's data only	☒	☐	☐	☒	☐	☑
Regulatory privacy defense and fines	☒	☒	☒	☒	☒	☐
Virus and malicious code transmission	☒	☐	☒	☒	☐	☑

☒ No coverage ☐ Possible coverage ☑ Coverage

The legal environment

- Data Breach definition varies by state law
  - 47 jurisdictions have specific breach notification laws
  - Differ as to how and when notification requirements are triggered
    - Risk of harm
    - Acquisition and access
- The definition varies by federal law
  - For example, HIPAA and HITECH
  - Attempts to pass federal data security breach legislation

The reach of states



Maryland Personal Information Protection Act Md. Code 14-3504

- Personal Information:
  - An individual's first and last name in combination with a:
    - Social Security number
    - Driver's license number
    - Financial account number or individual tax payer identification number
    - unless the information is encrypted, redacted, or otherwise rendered unusable.
- Security Breach: the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of personal information.

Maryland Personal Information Protection Act

NOTIFICATION REQUIRED

- Notification: After a good faith, prompt and reasonable investigation, if an entity determines that a reasonable chance that the data will be misused exists, entity must notify the affected consumers.

- Notice must be given to consumers as soon as reasonably practical following the investigation.

- Business may delay notification if requested by a law enforcement agency or to determine the scope of the breach, identify all affected individuals or restore the integrity of the system.

Maryland Personal Information Protection Act

NOTIFICATION REQUIRED

- Notice must be given in writing and sent to the most recent address of the individual, or by telephone to the most recent phone number. Notice may be sent via email if an individual has already consented to receive electronic notice or the business primarily conducts its business via the internet.

- Substitute Notice: A business can provide notice of a security breach by email, posting on its website and notice to statewide media if the cost of notice would exceed $100,000 or the number of consumers to be notified exceeds 175,000 individuals.

Maryland Notification Requirements:

- Description of the information compromised
- Contact information for the business, including a toll free number if the business has one
- Toll free numbers and addresses for each of the three (3) credit reporting agencies: Equifax, Experian and Trans Union
- Toll free numbers, addresses and websites for the Federal Trade Commission (FTC) and the Office of the Attorney General (OAG)
- A statement that the individual can obtain information from these sources about steps to avoid identity theft

PRINCETON UNIVERSITY
Office of Information Technology
701 Carnegie Center
Princeton, NJ 08540

28 February 2011

4

Mr. Doiuglas F. Gansler
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202-2202
Attn: Security Breach Notification

Dear Attorney General Gansler:

Please be advised that Princeton University was recently informed of a breach of security. On February 9, 2011, certain content contained on a local server maintained by the University's Neuroscience Department for internal review was inadvertently made publicly available on the Internet. The information on this server was removed from public view immediately upon discovery on February 16, 2011 and all cached copies of the information have been removed. The files on this server likely contained each graduate school applicant's name, social security number, visa information, date of birth, home address, telephone number, other biographical information included in the application, education history, employment history, publications, curriculum vitae, transcripts, letters of recommendation, and faculty evaluations.

At this time, Princeton is not aware of any improper use of the personal information contained in the files. It appears that seventy-four (74) individuals could have been affected, including four (4) individuals who are residents of your state. We have already begun to notify affected individuals in certain other states and plan to begin notifying the affected individuals in Maryland in the next several days. A draft copy of the notification that will be sent is attached.

As set forth in the letter, Princeton University takes this incident very seriously and has implemented additional quality controls regarding server management to avoid similar incidents in the future.

If you require any additional information on this matter, please contact me.

Sincerely,

Rita Saltz
Senior Policy Advisor
Office of Information Technology (OIT)
Princeton University

(609) 258-6066
rita@princeton.edu

Yale University

Office of the Vice President and General Counsel
PO Box 208255
New Haven, CT 06520-8255

Campus Address
Whitney Grove Square
2 Whitney Avenue, 6th fl.
New Haven, CT 06510
Telephone: 203 432-4949
Fax: 203 432-7960

August 9, 2011

635

VIA U.S. MAIL
Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Dear Sir or Madam:

Pursuant to M.D. Code, Com. Law § 14-3504, we are writing to notify you of a recent incident of unauthorized access to personal information supplied to Yale University involving Maryland residents.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On June 30, 2011, Yale was notified that an individual affiliated with Yale had searched his name on Google, and located and downloaded from a Yale hosted FTP server an electronic spreadsheet containing names and Social Security numbers. Upon investigation, Yale concluded that the computer file had been stored for 10 months in a way that left the information in the file searchable using Google.

Upon further investigation, Yale determined that the affected computer file was created in 1999 and was inadvertently moved to an insecure section of a computer server in July 2005. Although, from July 2005, the file was no longer fully protected from unauthorized public access, it could not be located using an ordinary Internet search engine. The situation changed in September 2010, when Google modified its search engine in a way that allowed it to search files stored on servers like the one holding the affected Yale file. As a result, between September 2010 and July 1, 2011, it was possible that information in the affected file, including Social Security numbers, might have been located through a Google search.

Other than the circumstance described above, Yale has no evidence that the affected file was accessed by any other unauthorized user.

NUMBER OF MARYLAND RESIDENTS AFFECTED

There are six hundred thirty five (635) individuals with Maryland addresses whose personal information was the subject of the incident. These individuals will shortly receive written notice via first class mail pursuant to M.D. Code, Com. Law § 14-3504. A copy of the form of notice to affected Maryland residents is attached hereto as Exhibit A.

STEPS TAKEN RELATING TO THE INCIDENT

As soon as Yale learned of the problem, the affected file was removed from the Yale's Google searchable computer and, at Yale's request, Google removed from its search engine references to the file. Yale has confirmed that this file is no longer accessible through Google. Based on our research, there is no evidence that any other major search engine, including Yahoo and Bing, could or did locate the file, and, therefore, information from the affected file would not have been displayed in any of their search returns.

At this time, Yale has no reason to believe this incident is likely to result in harm to affected consumers and, therefore, Yale has not reported this incident to law enforcement. As a precaution, however, Yale intends to offer credit warning services to affected consumers.

Yale is searching its servers for similar archival files, and it is reviewing its procedures regarding the storing of archival information and, as appropriate, may revise these procedures. Further, Yale will remind employees of the importance of protecting all files containing personal information, including archival files.

OTHER NOTIFICATION AND CONTACT INFORMATION

Yale will send similar notifications to any regulatory agent required in the other states where residents were affected. If you have any questions or need further information please contact the undersigned attorney, Harold Rose.

Respectfully Submitted,

Harold Rose
Associate General Counsel

Yeshiva University

Andrew J. Lauer, Esq.
Vice President for Legal Affairs,
Secretary and General Counsel

500 West 185th Street
Belfer Hall 1001
New York NY 10033
P: 212.960.0153
F: 646.417.7358
andrewlauer@yu.edu
www.yu.edu

December 28, 2010

18

By First Class Mail and E-mail

A. Hugh Williams
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Legal Notice of Information Security Breach

Dear Mr. Williams:

I write to inform you of a potential information security breach involving approximately eighteen residents of your state. On December 8, 2010, we learned that a flash drive containing a number of Albert Einstein College of Medicine ("Einstein") admission applications was lost following a staff meeting. Unfortunately, according to the Einstein Admissions Department, the flash drive contained certain applicant data including names, addresses, telephone numbers, Social Security numbers, and email addresses. We have conducted several searches for the flash drive but have been unable to locate it.

At this time, we have no reason to believe that any personal information has been or will be accessed or misused. Nonetheless, as a precaution, we are notifying all affected individuals via written letter to each through first class mail, and offering them the opportunity to enroll in a free credit monitoring service for one year. These notifications will begin mailing on or about December 29, 2010. A copy of the form of notice to affected individuals is attached for your reference.

If you have any questions or need further information regarding this incident, please do not hesitate to call me at 212.960.0153.

Very truly yours,

Andrew J. Lauer
Vice President for Legal Affairs, Secretary and General Counsel

Enclosure

RECEIVED
OFF OF THE ATTY GENERAL
2011 MAY -3 P 6:01

RECEIVED
OFF OF THE ATTY GENERAL
2011 MAY -3 P 11:34

SONY

Sony Network Entertainment

6080 Center Drive 10th Floor, Los Angeles, CA 90045 Telephone (310) 981-1500 Fax (310) 981-1600

Office of the Attorney General
Consumer Protection Division
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566
E-mail: Idtheft@oag.state.md.us

630,000

April 26, 2011

Dear Attorney General Gansler:

I am writing to notify you that between April 17 and 19, 2011, Sony Network Entertainment America Inc. ("**Sony**") experienced an illegal and unauthorized intrusion into our PlayStation Network and Qriocity platform. The intrusion compromised certain personal information about approximately 630,000 Maryland residents, including name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password, login, and handle/PSN online ID. It is also possible that profile data, including purchase history, and billing address (city, state, zip), and PlayStation Network/Qriocity password security answers may have been obtained. While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility. If a customer has provided his/her credit card data through PlayStation Network or Qriocity, out of an abundance of caution we are advising that such credit card number (excluding security code) and expiration date may also have been obtained.

In response to this intrusion, we have temporarily turned off PlayStation Network and Qriocity services, and we have engaged an outside, recognized security firm to investigate this incident and to assist us in our ongoing efforts to protect personal information. We have also quickly taken steps to enhance security and strengthen our network infrastructure by re-building our system to provide greater protection of our users' personal information.

We are now in the process of contacting relevant state authorities, including your agency. We also have begun preparations for notification to all affected individuals of the data loss. The residents will shortly be notified by email, website posting, and statewide media. A copy of the notification is attached. Please contact me right away at (310) 981-1509 or ajay.patel@us.sony.com in the event that you have any questions regarding this matter.

Sincerely,

Ajay Patel

Delaware Computer Security Breaches Statute

- Title 6, Section 12B-101

- Breach in security system means unauthorized acquisition of unencrypted computerized date that compromises security, confidentiality, or integrity of personal information maintained by an individual or commercial entity.
- An entity when it becomes aware of breach in the security of a system shall conduct in good faith a reasonable and prompt investigation
- Investigation in to the terms of the misuse of the information has occurred or reasonable likely to occur notice should be given as soon as possible to the affected Delaware resident

Delaware Computer Security Breaches Statute

- Notice must be made in the most expedient time possible without unreasonable delay
- Notice can be delayed pursuant to a law enforcement investigation
- An entity that maintains computerized data but does not own the data shall give notice to, and cooperate with, the owner of the information of any breach the security of the system immediately following discovery of the breach
- The Attorney General may bring an action in law or equity to address violations of this Chapter and for other relief that may be appropriate

District Of Columbia Consumer Security Breach Notification

- Chapter 38 § 28-3851
- Any individual or entity who discovers a breach in the security of its system shall promptly notify any District of Columbia resident whose personal information was included in the breach.
- Any individual who maintains or handles electronic data but does not own such data shall notify the owner or licensee of any breach in the security system in the most expedient time possible.
- If any person or entity is required to notify more than 1,000 persons of the breach that person shall also notify without unreasonable delay all consumer reporting agencies
- A notification can be delayed pursuant to a law enforcement agency request
- Any District of Columbia resident injured may institute a civil action to recover actual damages, the cost of the action, and reasonable attorney fees. Actual damages shall not include pain and suffering.

District of Columbia Data Breach Example

- Howard University Hospital notification to 35,000 patients
- In January 2012, contractor's personal laptop stolen
- The laptop was stolen from his vehicle and password protected
- No evidence of any patient files had been accessed
- The former had downloaded the files to a personal laptop which violated the privacy rules
- The date included names, addresses, social security numbers, identification numbers, medical records numbers, birth dates
- Notification letters were sent and identity theft alert coverage for one year was provided

Family Educational Rights and Privacy Act of 1974 (FERPA)

- Provides a student or former student the right to:
  - Inspect and review their education records
  - Amend those records
  - Have some control over the disclosure of information from those records
- FERPA applies to all educational institutions that are recipients of federal funding

Who is protected under FERPA?

- Students, regardless of age or parental dependency, who currently are or formerly have been enrolled in an institution of higher education
- Under specific defined conditions, parent of a student identified as a “dependent” for income tax purposes may have access to the student’s educational record
- A student who has applied but has not attended an institution is not protected by FERPA

What are educational records?

- Any record maintained by an institution or agent of the institution where a student can be personally identified
- FERPA does not require that certain records be kept
- Records may be in any medium (handwritten, computerized, etc.)
- Includes transcripts or other records obtained from a school in which a student was previously enrolled

FERPA – Breach notification

- FERPA does not require or recommend that an educational agency or institution notify students that information from their education records was stolen or otherwise subject to an unauthorized release
- FERPA does require an agency or institution to maintain a record of each disclosure
- Direct student notification is advisable only if the compromised data includes student Social Security numbers and other identifying information that could lead to identity theft

CONTACTS

- **David J. Shannon, Esq.**
  Chair, Technology, Media & Intellectual Property Practice Dept.
  bio | e-mail | website
  2000 Market St.
  Suite 2300
  Philadelphia, PA 19103

- John Farley, Vice President, Data Breach Consultant,Wells Fargo Insurance Services USA, Inc. | 330 Madison Avenue, 7th Floor New York, NY 10017

Phone: 212-209-0227 e-mail
john.farley@wellsfargo.com

Questions