



The
BUSINESS RECORDS MANAGEMENT
BULLETIN



A Service of **BUSINESS RECORDS MANAGEMENT**

1st Quarter 2008

DATA PROTECTION LEGISLATION

There are at least four pieces of legislation concerning personal data that were introduced in early 2007 in the U. S. Congress—one in the House, three in the Senate.

- HR 1685, Data Security Act of 2007
- S 239 RS, Notification of Risk to Personal Data Act of 2007
- S 495 RS, Personal Data Privacy and Security Act of 2007
- S 1178, Identity Theft Prevention Act

A first glance at their progression indicates they were each parceled out to multiple committees where they have been sitting since Spring 2007. (This is according to the legislative tracking system of the Library of Congress, www.libraryofcongress.gov, click on THOMAS.) Since all of these relate to privacy and security of personal data, it is interesting to note that “business goes on as usual.” Meaning the number of recorded security breaches of personal data continues unabated, with embarrassment and liability for large and small organizations throughout the United States and elsewhere.

The Privacy Rights Clearinghouse (www.privacyclearinghouse.org) has maintained a chronology of data security failures since 2005. During March, April and May 2007 while these four bills were being sent to committees, the Privacy Rights chronology racked up these numbers of incidents: March, 24; April, 29; May, 36. These ranged in size from 54 benefits letters with personal data of individuals in the AIDS Drug Assistance Program going to the wrong persons (March 2, California Department of Health Services) to 2,900,000 names and personal data on a disk that went



missing from a private vendor handling claims (April 10, Georgia Department of Community Health).

May 19 was not a good day. The Texas Commission on Law Enforcement Standards and Education discovered a computer was stolen with names and personal data on 230,000 Texas peace officers. The Illinois Department of Financial and Professional Registration had a server breached. It contained 300,000 names and personal data on banking and real estate professionals.

Incidents like these and others have propelled the need for legislation. What will each of these four bills do? Is there overlap? Are there differences? Here are some details about each bill.

H. R. 1685, the Data Security Act of 2007

This bill was introduced March 26, 2007 by Rep. Tom Price of Georgia to protect information relating to consumers, to require notice of security breaches, and for other purposes. It was referred to four committees and a subcommittee for study. One of its definitions states that the term “breach of data security” means the unauthorized acquisition of sensitive account information or sensitive personal information, with the exclusion that this does not include information that is not usable, that

is maintained or communicated in an encrypted, redacted, altered, edited, or coded form.

Under this bill, if a data breach is discovered and it is determined that this will cause substantial harm or inconvenience to those whose data is involved, the notification order is as follows:

- The agency or authority appropriate for this situation;
- An appropriate law enforcement agency;
- Any entity that owns or is obligated on a financial account relative to the breached data involved;
- All nationwide consumer reporting agencies if the breach involves 1,000 or more consumers; and
- All consumers whose data is involved.

The notice must include the type of information involved; the date or period of time when the breach occurred; actions taken by the owner of the data to restore security; and a summary of rights of identity theft victims as set forth in the Fair Credit Reporting Act. This bill also has provisions for protection of data by federal agencies and includes the law's relation to state regulations. According to THOMAS, nothing has happened with this bill since March 27, 2007.

S 239, Notification of Risk to Personal Data Act of 2007

This was introduced by Sen. Dianne Feinstein of California to require federal agencies, and persons engaged in interstate commerce, in possession of data containing sensitive personally identifiable information, to disclose any breach of such information. It was introduced January 10, 2007 and was placed on the Senate legislative calendar on May 31.

In general, this bill states that any agency or business entity involved in interstate commerce that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable data must notify any resident of the United States if their data has been, or is believed to have been, accessed or acquired. It sets forth the obligation for notice that must be given if the agency or business does not own the data, that is, if it is owned by a third party. There are stipulations on timeliness of notification and reasonable delay.

The bill also states that if a federal law enforcement

agency determines that notification would impede a criminal investigation, the notification will be delayed upon written notification from the law enforcement agency. Additionally, an agency or business entity can certify in writing that sending out notification of a breach will cause damage to national security or hinder a law enforcement investigation. This certification, with a factual basis for its use, must be provided immediately to the United States Secret Service. In reviewing this request, the Secret Service can ask for more information, and cooperation is mandatory.

There are some "safe harbor" provisions in this bill that exempt an agency or business from sending out a security breach notice—if a risk assessment concludes that no harm has happened, or will happen, to those whose data was at risk, and if the personal data was encrypted or rendered indecipherable through redaction, access controls or other such mechanisms.

S 495, Personal Data Privacy and Security Act of 2007

This was introduced by Sen. Patrick Leahy of Vermont on February 6, 2007. The purpose is to prevent and mitigate identify theft, ensure privacy, provide notice of security breaches, enhance criminal penalties, provide law enforcement assistance, and give other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

This bill also provides a safe harbor exemption for information that is encrypted or otherwise made indecipherable to those who should not have it. What sets it apart from the others is its focus on going after misusers of personal data, the bad guys. Section 1040 states that anyone who has knowledge of a security breach (that has not been qualified for an exemption) and conceals this fact "shall be fined under this title or imprisoned not more than 5 years, or both."

Furthermore, Section 103 addresses federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personal information. It states that the United States Sentencing Commission shall review and amend sentencing guidelines to reflect the serious nature of these offenses and penalties and the need to deter, prevent and punish such offenses.

With sympathy for the victims of identity theft, Leahy's bill deals with the effects of identity theft on

bankruptcy proceedings. An “identity theft victim means a debtor who, as a result of an identity theft in any consecutive 12-month period during the 3-year period before the date on which a petition is filed under this title, had claims asserted against such debtor.” “No judge, United States trustee (or bankruptcy administrator, if any), trustee, or other party in interest may file a motion under paragraph (2) if the debtor is an identity theft victim.”

S 1178, Identity Theft Prevention Act

This was introduced by Sen. Daniel Inouye of Hawaii on April 20, 2007. Its purpose is to strengthen data protection and safeguards, require data breach notification, and further prevent identity theft.

One provision details the steps to be taken if a security breach affects 1,000 or more persons. The breach should be reported to the Federal Trade Commission or other appropriate federal regulator, and all consumer reporting agencies should be notified as described in the Fair Credit Reporting Act. The FTC is to post a notice on its website concerning the breach showing the number of persons affected and the remedial action taken by the owner or user of the data. For breaches involving less than 1,000 individuals, and if there is not a risk of identity theft, the breach shall be reported to the FTC or other agency with the number of persons involved and type of information exposed.

The FTC can not publish such a report on its website nor disclose any personal information about the individuals.

This bill also states that a consumer may place a security freeze on his or her credit report by making a request to a credit reporting agency. There are several stipulations relative to non-release of information, release with authorization of the originating consumer, and the fact that a security freeze on a credit report may not be taken into account in determining the credit score of the consumer.

Relative to identity theft, there is a bill that was approved by the Senate in November 2007 titled S 2168, Identity Theft Enforcement and Restitution Act. It increases penalties, gives new tools to prosecutors, and assists victims in seeking restitution for the loss of time and money that identity theft brings with it.

Are you encrypting your data?

It is interesting to note that three of these bills specifically exempt personal data that is encrypted, redacted, altered, edited or coded. If you are not protecting the personal data files of your organization, you should be considering that step. Your storage contractor can help you get started on that major safeguard.

ARMA International’s 2nd Annual E-Discovery and Beyond Seminar:

Manage Your Electronic Data Risk, is a two day, interactive event being held March 31-April 1, 2008 in New York City at the Marriott Marquis in Times Square. The seminar is specifically designed for those who manage information, and to educate attendees on how to use the tools and processes needed to reduce risk while becoming more competitive and compliant as an organization.

Sessions will feature experts in the legal, records and information, and IT fields covering hot topics such as legal holds, risk management, ethics, and more. They will also demonstrate how to align efforts to create a successful discovery process within an organization for effective day-to-day business.

For the E-Discovery and Beyond seminar, ARMA International is pleased to have the assistance of the following corporate sponsors: CA, FTI Consulting, IBM, LexisNexis Applied Discovery, NextPage, and TAB. The association partner is the International Legal Technology Association (ILTA) and the luncheon will be provided by HP Invent/Clearwell.

For more information and to register for EDiscovery and Beyond visit:
www.arma.org/ediscovery

ARMA International Educational Foundation (AIEF) Announces 2008 Graduate Level Scholarship

The ARMA International Educational Foundation (AIEF) has established a scholarship program to encourage development of the international records and information management community with an appropriately educated records and information management workforce.

Graduate Level Scholarship

A Scholarship of \$3000 will be awarded annually, in the summer, to a full-time student entering the second year of a graduate records and information management program or equivalent library science or archival studies program which contains a significant number of records management and information courses at a recognized university or a college leading to a Masters degree or equivalent.

Eligibility and Application Process

Any student enrolled in a recognized graduate program who:

1. Provides evidence of the intention to continue with the second year of such a program.
2. Submits an outline of the courses and related papers completed in the first year;
3. Submits evidence of being a member in good standing of ARMA International or another nationally or internationally recognized information management association;
4. Provides evidence of having attained a grade average of 80% or a B average or higher in the first year of their graduate degree program as indicated by the submission of an official transcript;
5. Prepares a 1000 or more word research essay which thoroughly explores an aspect of records and information management studies. If deemed appropriate by the AIEF, further agrees to allow the AIEF to publish the essay;
6. Agrees to the terms and conditions of the Scholarship; Submits one hard copy of a letter of application, the documentation indicated above and three letters of reference from individuals able to comment on the applicant's academic performance involvement or

interest in the records and information management community and leadership abilities;

7. Applications are due by the end of April of 2008 and are to be submitted to:

Preston W. Shimer, FAI
Foundation Administrator
ARMA International Educational Foundation
1609 Terrie Drive
Pittsburgh PA 15241 USA

For further information, visit the Foundation Website <http://www.armaedfoundation.org/scholarship1.html>

Adjudication

The applications will be adjudicated by a committee of three Trustees of the AIEF, a member of the Board of Directors, ARMA International, and one non- Board or Trustee member drawn from the academic community. In addition, at least one member shall be a records or information management professional residing outside of the United States. A majority of the members voting for one applicant will be needed for the award to be made.

The scholarship will be announced on the AIEF Web site and at the 2008 ARMA International Conference following the determination of the award.

If, in the opinion of the adjudication committee, no applications received in a given year warrant an award, none will be given in that year. At this time a maximum of one scholarship will be awarded in any given year.

Payment

Payment will be made in two equal installments, at the beginning of each education term. Each check will be sent to the collegiate institution to which the successful applicant is attending within 15 days of receipt of a letter from the head of the relevant studies program indicating that the student has commenced full-time studies. Failure to submit such letters within 30 days of beginning of each term will result in the forfeiture of the scholarship.

Records

All records relating to the adjudication, except the name and address of the recipient and the student essay, are destroyed one year after the final payment is issued.

From time to time and due to a variety of circumstances including untimely or tragic death, planned giving or regular or one time donations, the AIEF may create scholarships, awards, or prizes which are suitable to the circumstances. These may be of varying duration depending on the level of funding and may be through the AIEF or in partnership with others, including, but not limited to records and information management education programs, and records and information management institutions, organizations and associations.

Funding

The AIEF will seek funding to support its scholarships, fellowships, awards and prizes as they are developed. The Foundation will establish a specific budgetary process to document such funding.

Funding will be sought from:

1. ARMA International donations
2. ARMA Chapter donations
3. Raffles and Drawings at Chapter functions and the annual ARMA International Conferences
4. Corporate donations
5. Memorial giving
6. Living wills
7. Partnerships
8. Other resources as appropriate

For additional information, contact:

Preston W. Shimer, FAI
Foundation Administrator
ARMA International Educational Foundation
1609 Terrie Drive
Pittsburgh PA 15241 USA
412-221-1736
Admin@armaedfoundation.org

Employee Profile



Chris Neefus is BRM's new Chief Executive Officer. Chris has worked in the services industry since 1978, bringing for more than 29 years of business services experience to BRM. Most recently, he was the Executive Vice President and Chief

Operating Officer for the North American operations of Iron Mountain Inc., based in Boston MA. His breadth of practical management experience positions Chris to offer strong business planning leadership to BRM.

Chris has a long history of business development and management responsibility beginning in New York with Time Sharing Resources Inc., Informatics Inc. (a wholly owned subsidiary of the Equitable Insurance Company) and Anacomp Inc., (a Fortune 500 technology services provider). Chris also acquired retail experience as the founder and President of Cobbler Ventures Ltd., a small chain of restaurants which he sold in 1989.

Chris and his wife Teresa enjoy spending time with their Golden Retriever "Tess" and vicariously reliving their college years through their two sons.

From the Office of the President

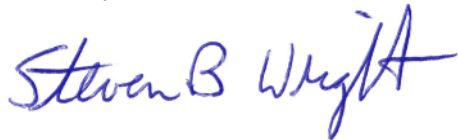
I am pleased to announce that I have formed a new company along with The Goldman Sachs Group, Inc. to acquire the assets of Business Records Management, Inc. This new company retains the BRM name as Business Records Management LLC. Under my continued management, BRM will service all accounts from the same facilities utilizing the same staff with no change to our operating procedures. Our existing Customer Service Team will continue to take calls and address requests as usual, and the terms and conditions of all existing contracts will remain the same.

Goldman Sachs has been involved with the information management business for a number of years and is proud to be part of such a valued brand name in the industry. We will continue to retain the BRM name as we improve and expand our business throughout North America. As a result of the transaction, we also welcome a new CEO, Chris Neefus, to the BRM family to pursue this growth strategy. I believe having Chris and the resources of Goldman Sachs at our disposal will benefit our customers, our company, and our employees alike. The growth of BRM will also bring additional benefits as we are able to increase our service offerings and continue to increase the quality of all services.

Both Chris and I personally look forward to the opportunities that lie ahead for ourselves and for BRM. We would like to take this opportunity to pledge our continued commitment to the success of your company and our ongoing partnership in servicing your needs.

I want to personally thank you for your business and I am confident that this transaction will strengthen our mission to be the premier business records management company.

Sincerely,



Steven B. Wright

Congratulations eNewsletter 1st Quarter Winners

Congratulations to **Linda Ammon** of Beaver Concrete & Gravel in Rochester, PA and **Robert Wise** of PerkinElmer Genetics Inc. in Bridgeville, PA. They both won restaurant gift certificates. On behalf of everyone at BRM, thanks again and we hope you have a great time dining out!



BUSINESS RECORDS MANAGEMENT
BRM Disaster Recovery Services

1018 Western Avenue
Pittsburgh, PA 15233
Voice: 412-321-0600
Fax: 412-321-5152
Web: www.businessrecords.com