

Excerpted from the Oklahoma Bar Journal, Vol. 80, No. 7, March 14, 2009, published by the Oklahoma Bar Association. Reprinted with permission.

Oklahoma's Security Breach Notification Act

By Eric L. Johnson

It seems like every week we see a report on the news or read a newspaper story about a data or security breach where a person's sensitive and personally identifying information, including name, address, Social Security number, credit card number and/or medical history, collected by a bank, company, credit union, hospital, law firm, university, state or federal government entity was released into the "wild" and/or obtained by the bad guys. A data or security breach of a system involves the exposure and/or theft of a person's sensitive personal information; often on a massive scale. The 2008 data breach tally from the Identity Theft Resource Center (ITRC), a nonprofit organization dedicated to the understanding and prevention of identity theft, puts the total number of security breaches through Nov. 25, 2008, at 585; an increase from the final total of 446 reported in 2007. These 585 security breaches resulted in the exposure of over 33 million records.¹ While this number may seem large, it is probably actually larger as the ITRC estimates that in more than 40 percent of breach events, the number of records exposed was not reported or fully disclosed by the breached entity.

The various types of entities that have reported security breaches generally fall into the following categories: (a) educational institutions (public and private colleges, universities and alumni organizations); (b) healthcare organizations (hospitals, healthcare services and healthcare insurers); (c) financial services companies (banks, credit card companies, credit unions, finance companies, insurance companies and investment services); (d) general businesses; and

(e) government agencies (federal, state and local governmental agencies).

The reported security breaches can then be categorized by the cause of the breach:

- **Hacking:** Illegal access through the Internet to data contained in a computer system by a person external to the breached entity (including viruses, Trojan horses and computer security loopholes);

- **Improper display or disposition:** Allowing sensitive personal information to be viewed by those who should not have access (for example, information bought by a fake business or sensitive information tossed into dumpsters);

- **Insider access:** An employee or contractor stealing or providing others with access to sensitive personal information held by his or her employer;

- **Lost backup:** Data storage media containing sensitive personal information lost in the process of transferring the media to another location;

- **Physical theft:** The theft of laptops, computer equipment, other computer storage devices or paper files; or

- **Not specified:** The specific cause of the breach was not publicly disclosed by the entity suffering the breach.

Oklahoma recently became one of 44 states² to enact security breach legislation that requires individuals or entities that own or license computerized data that includes personal information to notify Oklahoma residents of any breach of the security of the system if their personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person. Originally introduced in the 2nd Session of the 51st Legislature (2008) for the state of Oklahoma,³ Oklahoma H.B. 2245, titled the “Security Breach Notification Act” was signed by Gov. Henry on April 28, 2008. The act became effective on Nov. 1, 2008, and applies to the discovery or notification of a breach of the security of the system that occurs on or after that date. Note that Oklahoma has had a security breach statute on the books since 2006, but its scope was extremely limited.⁴ This article summarizes the salient provisions of the act and its requirements on Oklahoma individuals and entities.

APPLICABILITY

The act relates to identity theft and will affect all individuals (natural persons) or entities⁵ that own or license computerized data which includes personal information. In addition, the act also applies to any individual or entity that simply maintains computerized data which includes personal information that the individual or entity does not own or license. Personal information means the first name or first initial and last name in combination with and linked to any one or more of the following data

elements that relate to an Oklahoma resident — when the data elements are neither encrypted nor redacted:

- (a) Social Security number;

- (b) driver license number or state identification card number issued in lieu of a driver license; or

- (c) financial account number, credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident.

However, the term personal information does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

KEY DEFINITIONS

The act contains a few key definitions that are central to both the scope and application of the act:

A. Breach of the security of a system means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to any Oklahoma resident. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or the entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure;

B. Encrypted means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable;

C. Notice means:

- 1) written notice to the postal address in the records of the individual or entity;

- 2) telephone notice;
- 3) electronic notice; or
- 4) substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, or that the affected class of residents to be notified exceeds 100,000 persons, or that the individual or the entity does not have sufficient contact information or consent to provide notice as described above. Substitute notice consists of any two of the following:

(a) e-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;

(b) conspicuous posting of the notice on the Internet Web site of the individual or the entity if the individual or the entity maintains a public Internet Web site; or

(c) notice to major statewide media.

D. Redact means alteration or truncation of data such that no more than the following are accessible as part of the personal information: (a) five digits of a Social Security number, or (b) the last 4 digits of a driver license number, state identification card number or account number.

NOTIFICATION REQUIREMENTS

A. Individual or entity owns or licenses computerized data.

An individual or entity that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to

any Oklahoma resident whose unencrypted and unredacted personal information was or is *reasonably believed* to have been accessed and acquired by an unauthorized person and that causes, or the individual or entity *reasonably believes* has caused or will cause, identity theft or other fraud to any Oklahoma resident. Except as provided below, or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system, the disclosure must be made without unreasonable delay.

An individual or entity must disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such breach has caused or will cause identity theft or other fraud to any Oklahoma resident.

B. Individual or entity maintains computerized data owned or licensed by another.

An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license must notify the owner or licensee of the information of any breach of the security of the system as soon as practicable following discovery, if the personal information was or if the entity *reasonably believes* was accessed and acquired by an unauthorized person.

C. Delay of notice.

The required notice may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation or homeland or national security. Once the law enforcement agency determines that notifi-

“**Encrypted means transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key...**”



cation will no longer impede the investigation or jeopardize national or homeland security, the required notice must be made without unreasonable delay.

COMPLIANCE

The following will be deemed to be in compliance with the notification provisions of the act:

An entity that:

- (a) maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information and that is consistent with the timing requirements of the act if it notifies Oklahoma residents in accordance with its procedures in the event of a breach of security of the system; or
- (b) complies with the notification requirements or procedures pursuant to the rules, regulation, procedures, or guidelines established by the primary or functional federal regulator of the entity.

In addition, a financial institution⁶ that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice⁷ is deemed to be in compliance with the act.

PENALTIES AND REMEDIES

The act provides enforcement authority for violations of the act that result in injury or loss to Oklahoma residents to the attorney general or a district attorney in the same manner as an unlawful practice under the Oklahoma Consumer Protection Act (OCPA).⁸ Under the OCPA, the attorney general or district attorney may bring an action:

- (A) to obtain a declaratory judgment that an act or practice violates the OCPA;
- (B) to enjoin, or to obtain a restraining order against a person who has violated, is violating, or is likely to violate the OCPA;
- (C) to recover actual damages and, in the case of unconscionable conduct, penalties as provided by the OCPA, on behalf of aggrieved consumer, in an individual action only, for violation of the OCPA; or
- (D) to recover reasonable expenses and investigation fees.

In lieu of instigating or continuing an action or proceeding, the attorney general or a district attorney may accept a consent judgment with respect to any act or practice declared to be a violation of the OCPA. The consent judgment must provide for the discontinuance of the violation of the OCPA, may provide for the payment of reasonable expenses and investigation fees incurred, and may include a stipulation for restitution and for specific performance. Such consent judgment will not operate as an admission of the violation unless the judgment does so by its terms. The consent judgment must also be approved by the court and entered as judgment, and once such approval is received, any breach of the conditions of the consent judgment shall be treated as a violation of the court order.

In addition, the attorney general or a district attorney may investigate if they have reason to believe a violation has occurred and an investigation is in the public interest. The investigation demand may include production of documents. Finally, subpoenas may be issued and hearings may be held.

A violation of the act by a state-chartered or state-licensed financial institution is enforceable exclusively by the primary state regulator of the financial institution. Otherwise, the attorney general or a district attorney will have exclusive authority to bring an action under the act for either actual damages or a civil penalty not to exceed \$150,000 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.

CONCLUSION

There are a vast number of different risks associated with data or security breaches including loss of consumer confidence, possible litigation and regulatory enforcement. As the incidences of data or security breaches are on the rise, it appears that the criminal population may be attacking and stealing more data from entities. Therefore, it is important for individuals and entities that own, license or maintain computerized data to take a look at their information privacy and security policies and the way they handle personal information, from securing data within the organization, to dealing with third parties, such as business partners and vendors, in order to protect consumers against identity theft and maintain consumer confidence. Finally, the individual or entity should also develop and implement a

response program in compliance with the act that includes procedures to notify consumers about incidents of unauthorized access to information that causes, or the individual or entity reasonably believes has caused or will cause, identity theft or other fraud to Oklahomans.

1. Available at: <http://idtheftmostwanted.org/ITRC%20Breach%20Report%202008.pdf>.

2. The other states that have enacted some form of security breach legislation are: Alaska (2008 H.B. 65); Arizona (Ariz. Rev. Stat. § 44-7501 (2007 S.B. 1042, Chapter 23)); Arkansas (Ark. Code § 4-110-101 et seq.); California (Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82); Colorado (Colo. Rev. Stat. § 6-1-716); Connecticut (Conn. Gen Stat. 36a-701(b)); Delaware (Del. Code tit. 6, § 12B-101 et seq.); Florida (Fla. Stat. § 817.5681); Georgia (Ga. Code §§ 10-1-910, -911); Hawaii (Haw. Rev. Stat. § 487N-2); Idaho (Idaho Code §§ 28-51-104 to 28-51-107); Illinois (815 ILCS 530/1 et seq.); Indiana (Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq.); Iowa (2008 S.F. 2308); Kansas (Kan. Stat. 50-7a01, 50-7a02); Louisiana (La. Rev. Stat. § 51:3071 et seq.); Maine (Me. Rev. Stat. tit. 10 §§ 1347 et seq.); Maryland (Md. Code, Com. Law § 14-3501 et seq.); Massachusetts (2007 H.B. 4144, Chapter 82); Michigan (Mich. Comp. Laws § 445.61 et seq.); Minnesota (Minn. Stat. §§ 325E.61, 325E.64); Montana (Mont. Code § 30-14-1701 et seq.); Nebraska (Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807); Nevada (Nev. Rev. Stat. 603A.010 et seq.); New Hampshire (N.H. Rev. Stat. §§ 359-C:19 et seq.); New Jersey (N.J. Stat. 56:8-163); New York (N.Y. Gen. Bus. Law § 899-aa); North Carolina (N.C. Gen. Stat. § 75-65); North Dakota (N.D. Cent. Code § 51-30-01 et seq.); Ohio (Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192); Oklahoma (Okla. Stat. § 74-3113.1 and 2008 H.B. 2245); Oregon (2007 S.B. 583, Chapter 759); Pennsylvania (73 Pa. Stat. § 2303 (2005 S.B. 712, Act 94)); Rhode Island (R.I. Gen. Laws § 11-49.2-1 et seq.); South Carolina (2008 S.B. 453, Act 190); Tennessee (Tenn. Code § 47-18-2107); Texas (Tex. Bus. & Com. Code § 48.001 et seq.); Utah (Utah Code §§ 13-44-101, -102, -201, -202, -310); Vermont (Vt. Stat. tit. 9 § 2430 et seq.); Virginia (2008 S.B. 307, Chapter 566); Washington (Wash. Rev. Code § 19.255.010); West Virginia (2008 S.B. 340, Chapter 37); Wisconsin (Wis. Stat. § 895.507); Wyoming (Wyo. Stat. § 40-12-501 to -501); District of Columbia (D.C. Code § 28-3851 et seq.); Puerto Rico (2005 H.B. 1184, Law 111).

3. 2008 Okla. Sess. Law Serv. Ch. 86 (H.B. 2245).

4. 74 O.S. § 3113.1. This security breach statute is only applicable to a state agency, board, commission or other unit or subdivision of state government that owns or licenses computerized data that includes personal information.

5. Entities (or Entity) are defined rather broadly and include corporations, business trusts, estates, partnerships, limited partnerships, limited liability partnerships, limited liability companies, associations, organizations, joint ventures, governments, governmental subdivisions, agencies, or instrumentalities, or any other legal entity, whether for profit or not-for-profit.

6. Any institution the business of which is engaging in financial activities as defined by 15 U.S.C. § 6809. In general, companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance.

7. 70 Fed. Reg. 15736 (March 29, 2005).

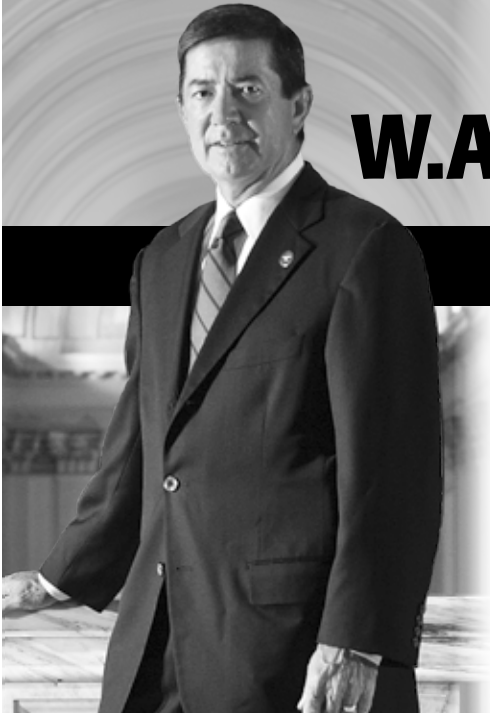
8. 15 O.S. § 751 et seq.

ABOUT THE AUTHOR



Eric L. Johnson is a shareholder with Phillips Murrah PC. He has 15 years of experience providing commercial and consumer credit compliance advice on federal and state laws and regulations. He is a registered lobbyist, an adjunct professor of consumer law for Oklahoma City University School of Law and chairs the Legal Committee for the National Automotive Finance Association. He is a frequent speaker and author on consumer financial services issues.

THE UNIVERSITY OF TULSA COLLEGE OF LAW CONGRATULATES...



The Honorable W.A. Drew Edmondson

2009 Alumnus-In-Residence

We are proud to recognize Drew Edmondson for his professional accomplishments and engaging law students through the Alumnus-in-Residence program.



www.law.utulsa.edu

The University of Tulsa is an equal employment opportunity/affirmative action institution.