

**TEXAS AG SUIT AGAINST RADIO SHACK FOR  
ALLEGED VIOLATION OF  
2005 TEXAS IDENTITY THEFT LAW  
MANDATES  
REMINDERS BUSINESSES OF EXPANDING  
DATA PROTECTION AND IDENTITY THEFT  
RISKS & LIABILITIES**

Tuesday, April 10, 2007

Texas Attorney General Greg Abbott last week announced that he had filed a lawsuit against Fort Worth-based Radio Shack for allegedly violating state identity theft laws. The lawsuit stems from an alleged incident last month in which thousands of consumer records, including social security and credit card numbers, were found dumped in a trash bin outside of a store in Portland, Texas. Attorney General Abbott's announcement is one of the latest in the ongoing series of announced legal actions against businesses in Texas and nationwide based upon alleged improper protection, use or disposal of sensitive personal health care, financial or other data about employees, customers or others.

The 2005 Texas law makes not protecting consumer information an offense that can result in fines of up to \$50,000 per violation. It also requires businesses to take specific steps to protect data, obligates businesses whose data security protections are breached to provide certain notifications to individuals whose personal data is breached, and guarantees other important rights for consumers. Like similar laws enacted in California and a growing number of other states, the Texas identity theft statute requirements supplement already existing federal privacy and data security mandates such as the Fair and Accurate Credit Transactions Act (FACTA), the Health Insurance Portability & Accountability Act, and various other federal laws.

The announced litigation adds Radio Shack to Choicepoint, LexisNexis, Bank of America, the Internal Revenue Service, the Veterans Administration and a host of other organizations who are facing civil or criminal consequences from failure to properly safeguard, restrict use or dispose of sensitive data under a ever-broadening range of federal and state laws and regulations. These and other widely reported legal actions provide important reminders to all U.S. businesses, employers and employee benefit plans about the importance of using appropriate processes to safeguard and restrict the use of sensitive health care, financial, and other confidential personal and business information collected, accessed or maintained from employees, vendors and others in the course of their operations. They also highlight the need to take appropriate steps to minimize their exposure to personal identity theft and other cybercrime scams by employees, business partners and others, who may attempt to misuse this sensitive data.

As demonstrated by the claims against Radio Shack and others, businesses as employers and otherwise, employee benefit plans and their fiduciaries and vendors face rising identity theft and cybercrime exposures and expanding state and federal cybercrime prevention mandates to secure their personally identifiable human resources and employee benefit data, customer and prospect data and other sensitive information. Meanwhile, businesses increasingly are forced to deal with a variety of practical human resources and fraud concerns that commonly arise when their business, employee benefit plan or individual employees are victimized by an identity theft, cybercrime or other data security breach.

Businesses and other organizations interested in learning more about what their organizations should do to manage their identity theft, data security and cybercrime risks and liabilities can find helpful information in a series of articles authored by Cynthia Marcotte Stamer. Ms. Stamer has authored numerous publications addressing these and related data security and privacy concerns including her articles on "Keeping Lists Within The Law" and "Establishing a Data-Protection Policy" recently published in the March and April, 2007 issues of Western Association News Magazine. She also is the author of "Chapter 35 -Medical Privacy" published in ERISA Litigation (BNA) (2006-2004); "Personal Identity Management" published in the May, 2005 issue of MD News; "Cybercrime and Identity Theft: Health Information Security Beyond HIPAA," published in the May, 2005 issue of ABA Health eSource; "Privacy and Securities Standards - A Brief Nutshell," published in the February, 2005 issue of the BNA

Journal of Tax Management & Compensation; "Employers face new health plan privacy rules required by HIPAA," published in the February 13, 2004 issue of the Houston Business Journal and a plethora of other training programs and other materials. Many of these and other helpful materials are available for review under the Publications link at located <http://cynthiastamer.com/articles.asp> or by contacting Ms. Stamer via e-mail or telephone.

For specific information about your organization's specific responsibilities under the 2005 Texas identity theft law or other relevant federal or state laws and regulations, please contact Ms. Stamer.

We hope that this information is useful to you. If you have questions about your company's privacy and security risk and exposures, or other human resources, employee benefit or other operational risks or internal controls practices, or to request publications, information about upcoming programs, or other materials, please contact: Cynthia Marcotte Stamer, P.C., Member, Glast, Phillips & Murray, P.C., 2200 One Galleria Tower, 13355 Noel Road, LB 48, and Dallas, Texas 75240. Telephone (972) 419-7188. E-mail [cstamer@gpm-law.com](mailto:cstamer@gpm-law.com).

For other helpful resources and information about data security and HIPAA, employee benefits and human resources matters, go to [CynthiaStamer.com](http://CynthiaStamer.com) or contact Ms. Stamer. If you or someone else you know would like to receive future Alerts or announcements about other developments, publications or programs, please be sure that we have your current contact information – including your preferred e-mail – by registering on our website at [cynthiastamer.com](http://cynthiastamer.com) or by providing that information to us via telephone, fax or e-mail using the above contact information.

### IMPORTANT NOTICES REGARDING THIS COMMUNICATION

This publication is provided by Cynthia Marcotte Stamer, P.C. for general informational and educational purposes to clients and other interested persons. Neither its distribution to any party nor any statement or information it contains is intended to or shall be construed as establishing an attorney-client relationship or to constitute legal advice. Readers also are cautioned that the information in this publication may not apply to all situations. Consequently, readers must not rely upon this publication or information it contains as a substitute for competent individualized legal advice about the specific circumstances of the reader. If you have received this publication in error or do not wish to receive these in the future, please notify us of your preferences to the attention of Ms. Stamer via email, fax, regular mail or telephone.

**REMINDER ABOUT ELECTRONIC COMMUNICATION SECURITY:** E-mail and other electronic communication may not be secure unless appropriate encryption methods are used. Therefore, they may present heightened risks of security breaches of the communication. Electronic communications also generally are subject to discovery on the same terms as other communications. Please consider carefully these concerns before communicating by e-mail or other electronic means. If you wish for us to communicate with you by means other than e-mail or wish for us to arrange for encryption of our e-mail communications, please contact us at 972.419.7188.

**IMPORTANT NOTICE REGARDING TRANSMISSIONS OF PROTECTED HEALTH INFORMATION:** Protected Health Information (PHI) is individually identifiable health information. Any PHI contained in this e-mail is intended only for the intended recipient and is disseminated subject to the understanding that all requirements of HIPAA and other applicable laws for this disclosure have been met. If this communication contains PHI, you are receiving this information subject to the obligation to maintain it in a secure and confidential manner. Re-disclosure without additional consent or as permitted by law is prohibited. Unauthorized re-disclosure or failure to maintain confidentiality could subject you to penalties as described in state/federal law. If you are not the intended recipient, you are hereby notified that any disclosure, copying or distribution of this information is strictly prohibited. If you have received this message in error, please notify the sender immediately to arrange for return or destruction.

**ANTISPAM NOTICE:** Pursuant to the CAN-SPAM Act, this communication may be considered an advertisement or solicitation. If you would prefer not to receive future marketing and promotional mailings or to provide other directions about the tailoring of messages directed to your attention, please send an email with the word "unsubscribe" in its subject heading to [cstamer@gpm-law.com](mailto:cstamer@gpm-law.com) or otherwise contact us via postal mail to Cynthia Marcotte Stamer, Member, Glast, Phillips, & Murray, P.C., 2200 One Galleria Tower, 13355 Noel Road, L.B. 48, Dallas, Texas, 75240, Attention: Cynthia Marcotte Stamer, P.C.

**CIRCULAR 230 NOTICE:** The following disclaimer is included to comply with and in response to U.S. Treasury Department Circular 230 Regulations. ANY STATEMENTS CONTAINED HEREIN ARE NOT INTENDED OR WRITTEN BY THE WRITER TO BE USED, AND NOTHING CONTAINED HEREIN CAN BE USED BY YOU OR ANY OTHER PERSON, FOR THE PURPOSE OF (1) AVOIDING PENALTIES THAT MAY BE IMPOSED UNDER FEDERAL TAX LAW, OR (2) PROMOTING, MARKETING OR RECOMMENDING TO ANOTHER PARTY ANY TAX-RELATED TRANSACTION OR MATTER ADDRESSED HEREIN.

