Cynthia Marcotte Stamer's
RISK MANAGEMENT & COMPLIANCE E-NEWS

NY AG CUOMO ANNOUNCEMENT OF FIRST SETTLEMENT AGREEMENT FOR VIOLATION OF NY SECURITY BREACH NOTIFICATION LAW
LATEST REMINDER OF EXPANDING DATA PROTECTION AND IDENTITY THEFT RISKS & LIABILITIES

April 30, 2007

The April 26 announcement by New York Attorney General Andrew M. Cuomo that that it had negotiated the first settlement with a business charged under New York's Information Security Breach and Notification Law is the latest reminder to business leaders of their expanding data security and identity theft responsibilities under federal and state law. The announced New York settlement resolves state law claims brought against CS Stars for alleged violations of a New York identity theft protection law that among other things requires that businesses provide prompt notification to individuals whose personal data may have been compromised by a data security breach. The announced New York settlement follows the announcement earlier this month by Texas Attorney General Greg Abbott of his department's filing of two lawsuits against Radio Shack and CVS Pharmacies for alleged violation of a two-year old Texas Identity Theft statute. Additional details about these lawsuits and other tips to help businesses mitigate their exposure to these data security breach liabilities and other related information is available at cynthiastamer.com

According to the April 26, 2007 announcement by Cuomo, the settlement settles charges brought against CS STARS arising from its delay in reporting a data security breach affecting personal data of approximately 540,000 New Yorkers in May, 2006. As in Texas, California and a growing number of other states, New York law requires that business provide certain notifications of breaches of the security of private information and take other steps to safeguard sensitive personal information collected or maintained by the business about third parties. Under New York's Information Security Breach and Notification Law, for instance, any business that maintains private information that it does not own must notify the owner of the data of any security breach “immediately following discovery” of the breach and must notify all affected consumers in the “most expedient time possible.” Additionally, the business also must notify the New York Attorney General’s office, the Consumer Protection Board, and the state office of Cyber Security.

According to the Cuomo announcement, a CS STARS employee noticed on May 9, 2006 that a computer owned by the New York Special Funds Conservation Committee (“Special Funds”) was missing. The Special Funds computer held personal information, including the names, addresses, and social security numbers of thousands of recipients of workers’ compensation benefits. The Special Funds is a not-for-profit organization created to assist in providing benefits to workers under the New York Workers' Compensation Law.

CS STARS waited more than two months before notifying Federal and state officials of the breach and nearly three months before notifying the Special Funds or the affected consumers of the breach. CS STARS gave notice of the breach to Special Funds and the Federal Bureau of Investigations (FBI) of the security breach on June 29, 2006 and to the New York Attorney General’s office, the Consumer Protection Board, and the state office of Cyber Security the following day.

After notifying government officials of the breach, CS STARS continued to delay notification of the approximately 540,000 potentially affected New York consumers about the breach at the request of the FBI. On July 25, 2006, the FBI determined that the computer had been stolen by an employee of a cleaning contractor, and the missing computer was located and recovered.

In announcing the settlement, Attorney General Cuomo said, “This company had sufficient cause to believe that the private information contained in the missing computer had been acquired by a person without valid authorization.

Had the sensitive personal information fallen into the hands of criminals with the intent of identity theft, there would have been ample time to victimize hundreds of thousands of consumers. The law requires prompt notice to prevent such disastrous results."

Without admitting to any violation of law and cooperating fully with the Attorney General's investigation, CS STARS agreed to comply with the law and ensure that proper notifications will be made in the event of any future breach. The company also agreed to implement more extensive practices relating to the security of private information. CS STARS will pay the Attorney General's office $60,000 for costs related to this investigation.

As demonstrated by the state law claims against CS STARS, Radio Shack, CVS Pharmacies, and a host of others, businesses 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. The settlement agreement announced by Attorney General Cuomo provides helpful insights to the types of protective actions that the State of New York expects businesses to take to protect sensitive personal data under the New York law. More information on the New York State Information Security Breach and Notification Act can be found at: http://www.cscic.state.ny.us/security/securitybreach. Businesses operating in New York are encouraged to take prompt action to evaluate their responsibilities and liabilities in light of this information.

In addition to the specific responsibilities that may apply in New York or other states, businesses also generally are subject to a variety of data security prevention and other related responsibilities under various federal laws. 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.

If you have additional questions about your company's privacy and security risk and exposures under applicable federal or state laws, 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.

We hope this information is useful to you. For other helpful resources and information about data security and other risk management matters, go to 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 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 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.