Advisory
WHITE-COLLAR DEFENSE, INVESTIGATIONS & CORPORATE COMPLIANCE
PRACTICE GROUP | OCTOBER 2008

WIGGIN AND DANA
Counsellors at Law

New Data Privacy Law in Connecticut Imposes Stiff Penalties

A new Connecticut data privacy law, Public Act No. 08-167 titled An Act Concerning the Confidentiality of Social Security Numbers, became effective on October 1, 2008. The new law requires people and businesses to protect personal data and imposes both requirements and restrictions with respect to the handling of Social Security numbers. Intentional violations of the new law can result in a fine of $500 per Social Security number improperly disclosed, with a cap of a $500,000 fine for a single event involving the improper disclosure of multiple Social Security numbers.

Specifically, the new law requires that:

- anyone in possession of "personal information" is required to protect it from misuse by others and to dispose of "personal information" in such a way as to prevent misuse; and
- anyone who acquires Social Security numbers must also institute a "publicly displayed" privacy protection policy.

The law defines "personal information" as "information capable of being associated with a particular individual through one or more identifiers," such as "a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number," and other identifying numbers. "Personal information" does not include publicly available information "that is lawfully made available to the general public from federal, state or local government records or widely distributed media." The privacy protection policy called for by the new law must protect the confidentiality of, prohibit disclosure of, and limit access to Social Security numbers, and must be published or publicly displayed.

The new legislation raises some interesting questions. First, the geographic scope of the Act does not appear to be limited to safeguarding personal information of state residents, nor is its reach explicitly limited to persons and businesses operating in the state of Connecticut. As a result, out-of-state businesses and individuals could face penalties under the Act if any nexus permitting jurisdiction in Connecticut is established. Second, the Act explicitly exempts "unintentional" conduct. Thus, factual questions concerning whether specific conduct was "intentional" or "unintentional" will be resolved by regulators, in the first instance. Take this hypothetical example: A company is well aware that its data handling practices are deficient, but the company concludes that the expense of improving its systems is too great. As a consequence of the company's deficient systems, a file with thousands of Social Security numbers is inadvertently transferred to a third party, who, of course, promptly informs the media. In that case, the particular transfer was unintentional, but the practice was not. It

WIGGIN AND DANA
Counsellors at Law

remains to be seen whether such reckless disregard for the risk of a data loss will be labeled as "unintentional." Finally, the Act directs that fines paid be deposited into the "privacy protection guaranty and enforcement account" established by Senate Bill No. 30 to reimburse victims of identity theft. However, Senate Bill No. 30 was never passed, so it is unclear how fines paid will be expended.

Connecticut's new law is consistent with a developing trend in privacy protection law following enforcement actions by the Federal Trade Commission ("FTC") charging that companies risked customers' personal information as a result of inadequate privacy policies and practices. These enforcement actions have resulted in consent agreements with hefty fines and governmental oversight. In addition, the United States Department of Justice ("DOJ") recently announced indictments of almost 50 people, who were charged with computer fraud and identity theft related to the theft, or attempted theft, of electronically-stored personal information.

Both Connecticut's new data privacy law and recent enforcement actions taken by the FTC and prosecutions initiated by the DOJ demonstrate that companies dealing with personal information – belonging to customers and belonging to employees – must develop a privacy policy and implement practices to protect personal information. Such practices should include identification of information collected, employee training, encryption where possible, proper disposal of materials, and collection and continued storage of only the minimal amount of information needed.

If you would like more information or guidance in dealing with Connecticut's new law or any other privacy issues, please contact from our White Collar Defense, Investigations, and Corporate Compliance practice group:

Scott D. Corrigan
212.551.2605
scorrigan@wiggin.com

James I. Glasser
203.498.4313
jglasser@wiggin.com

Joseph W. Martini
203.498.4310
jmartini@wiggin.com

Or from our Privacy and Data Security practice group contact:

Mark W. Heaphy
203.498.4356
mheaphy@wiggin.com