



**TORTS &  
PRODUCTS  
LIABILITY  
DEFENSE**

Thomas B. Cronmiller  
585.295.4424  
tcronmiller@hblaw.com

Gary H. Abelson  
Jessica M. Baker  
Nikki L. Baldwin  
Frank V. Balon  
Robert A. Barrer  
Neil D. Breslin  
Samuel J. Burruano  
David B. Cabaniss  
Brian D. Casey  
John R. Casey  
Linda J. Clark  
David M. Cost  
Timothy J. DeMore  
Nicholas J. DiCesare  
Erica M. DiRenzo  
Charles Z. Feldman  
Michael E. Ferdman  
William C. Foster  
John P. Gaughan  
Alexandra George  
Kevin P. Glasheen  
Kevin M. Hayden  
David M. Hehr  
Matthew J. Larkin  
George G. Mackey  
Brian G. Manka  
Dennis R. McCoy  
Thomas J. O'Connor  
Michael A. Oropallo  
Scott M. Pechaitis  
Alan R. Peterman  
Scott P. Rogoff  
Paul A. Sanders  
Tara J. Sciortino  
Robert M. Shaddock  
Matthew J. Skiff  
Michael J. Smith  
Stephen H. Volkheimer  
Mark T. Whitford  
Angela C. Winfield

## Exposure for Identity Theft: Data Privacy Breaches and State and Federal Data Security Laws

Identity theft raises serious and potentially costly risks for businesses and individuals. Advances in computer technology have made it possible for detailed personal information to be compiled and shared more easily than ever. However, the risks of data breaches and corresponding legal obligations affect all businesses, regardless of their size.

Businesses that experience a data security breach can lose the trust of their customers, suffer impaired goodwill and lost revenue, face stiff civil penalties, and be exposed to class action lawsuits. We anticipate that data privacy and security legislation and case law will be one of the hottest emerging legal issues in the coming year. Legal actions for such breaches are likely to increase over the coming months. Many questions surround this new quasi-tort litigation, including defining the elements of a cause of action, the extent of the duty owed by businesses and the circumstances in which a breach can result in monetary damages, and the kind of damages that will be recoverable.

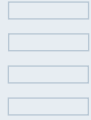
One source of exposure flows from state and federal data security laws. In response to highly publicized security breaches involving personal financial data, personnel records and bank information, state and federal governments have taken action to enhance regulations governing the storage and transmission of sensitive personal information.

The States of New York, Massachusetts, Connecticut, California, Florida, Michigan, Kentucky, Kansas, and Pennsylvania have introduced, reintroduced, or amended legislation of this kind:

- In New York, proposed amendments to the Information and Security Breach and Notification Act (2005) will mandate data security and encryption measures, update and refine definitions of "encryption" and "private information", and establish a general encryption standard as a safe harbor. The proposed bill also requires businesses and state agencies to implement and maintain reasonable security safeguards appropriate to the nature of the information and to prevent unauthorized access to or unauthorized destruction, use, modification, or disclosure of private information. In addition, the proposed bill requires notification to the State Attorney General of certain breaches and provides that persons, businesses and State entities that "experience breaches in the security of computerized data affecting more than 500,000 persons would be required to provide a second notification describing the steps taken to mitigate the effects of the breach."
- The Kentucky bill requires government agencies to protect all personal data under the Gramm-Leach-Bailey Act.
- The Michigan bill introduces a state version of the Federal Trade Commission's "Red Flags Rule" and requires creditors to implement programs aimed at spotting "red flags" of possible identity theft.
- The Connecticut law penalizes individuals and businesses that intentionally or willfully fail to protect personal information such as Social Security numbers, driver's license numbers, insurance policy account numbers, credit card numbers and bank account information.

*(Continued on back)*

Hiscock & Barclay is a full service, 200-attorney law firm, with offices throughout the major cities of New York State, as well as in Boston, Washington, D.C. and Toronto. We provide comprehensive legal and business counsel to a diverse client base in 29 specialized practice areas with statewide and regional expertise as well as with national and international capabilities.



- Commercial Litigation
- Construction & Surety
- Corporate
- Creditors' Rights
- Economic & Project Development
- Energy & Utilities
- Environmental
- Financial Institutions & Lending
- Health Care & Human Services
- Immigration
- Indian Law
- Insurance Coverage & Regulation
- Intellectual Property & Technology
- Intellectual Property Litigation
- International Business
- Labor & Employment
- Lobbying & Election Law Compliance
- Media & First Amendment Law
- Municipal & Land Use
- Professional Liability
- Public Finance
- Real Estate
- Real Property Tax & Condemnation
- Regulatory
- Sports & Entertainment
- Tax
- Telecommunications
- Torts & Products Liability Defense
- Trusts & Estates

Violators are subject to civil penalties of \$500 per violation with a \$500,000 cap per event. The same penalty applies for the intentional failure to properly destroy, erase or make unreadable during disposal of records. The law does not apply to public entities and does not impose fines on negligent or unintentional violators.

- Recent revisions to the data security regulations in Massachusetts focus on a “risk based” approach which allows those covered by the regulations to customize their security programs to the size, scope, type of business and volume of personal information retained. The changes were made, primarily, to reduce the burdens on small businesses who either do not maintain a large amount of personal data or who may not have the resources to develop advanced data security safeguards. As of today, businesses have until March 1, 2010 to comply.

The United States Congress is also considering adopting federal legislation which would preempt this patchwork of state privacy rules. Though similar bills have languished for years, two bills passed through the Senate Judiciary Committee in November 2009 and now face a full vote in the Senate.

The proposed **Personal Data Privacy and Security Act** (S.1490) sets standards for protecting sensitive personally identifying information, imposes civil penalties for those who fail to protect that information, and imposes criminal penalties to those who intentionally conceal a security breach that they have a duty to report.

If passed, the bill would preempt most state data security laws and mandate the implementation of a comprehensive data security program for all businesses that maintain “personally identifiable information” of 10,000 or more individuals. Affected businesses would be required to assess internal data security, enact policies and protocols to reasonably manage those risks and detect breaches of security, and regularly assess the effectiveness of their controls.

In its current form, S.1490 includes a uniform federal data breach notification requirement “without unreasonable delay” to the affected individuals and to prominent media outlets in instances where the personal information of 5,000 or more individuals have been exposed. The bill prohibits the dismissal of Chapter 7 bankruptcy cases where the debtor is a victim of identity-theft. The bill also includes a “risk of harm” threshold which creates an exception to the notification requirement where there is no significant risk that the breach would result in harm. Covered businesses are entitled to a statutory presumption that no harm is likely to occur from a breach where encryption, redaction and other industry-standard controls are used.

Failure to comply with the provisions of the federal bill carries serious civil penalties:

- Failure to institute a comprehensive security program - \$5,000 per violation per day (the amount is doubled if it was a intentional violation), capped at \$500,000 per violation and
- “Failure to timely notify individuals affected by a reportable breach - \$1,000 per day per individual (double for intentional violations) with a cap of \$1,000,000 per violation.

Additionally, the bill makes it a federal crime for intentionally and willfully “concealing” a reportable breach and designates the unauthorized access of sensitive personally identifiable information as fraud, subjecting violators to racketeering charges.

A companion bill, the **Data Breach Notification Act** (S.139) requires federal agencies and businesses engaged in interstate commerce to notify individuals whose personal information is exposed unless doing so would harm national security or hinder law enforcement efforts. This proposed bill also requires that the Secret Service be notified in the event that the records of more than 10,000 individuals are accessed or if the database affected contains the records of more than 1,000,000 people, is a federal government database, or involves national security or law enforcement. ■

*If you require further information regarding the information presented in this Legal Alert and its impact on your organization, please contact any of the members of the Practice Area listed on the front of this Alert.*