VENABLE® LLP

Cybersecurity Alert

February 2013

Maryland Cybersecurity-Related Legislative Developments

AUTHORS

Michael J. Baader
Anthony J. Rosso
Dismas Locaria
Ryan M. Sweigard

RELATED PRACTICES

Privacy and Data Security
Legislative and Government Affairs
Domain Names and Cyber Protection
Communications

ARCHIVES

2013 2009 2005
2012 2008 2004
2011 2007 2003
2010 2006

The Maryland State Senate is considering several cybersecurity-related bills to advance the state's efforts to be the epicenter for cybersecurity. Maryland has already enacted several measures to foster cybersecurity companies and their technologies. State Senator Catherine E. Pugh and the Commission on Maryland Cybersecurity Innovation and Excellence have introduced four bills in the current legislative session aimed at protecting Maryland citizens from cyber intrusion and/or data breaches. This alert provides a brief summary of the proposed legislation.

SB 859 Maryland Personal Information Protection Act – Revisions

SB 859 amends the duties imposed on private businesses under Maryland's Personal Information Protection Act (PIPA) regarding keeping, securing, and destroying records that contain personal information of customers and response and notification in the event of a data breach. SB 859 increases the duties for private businesses by expanding the definition of customer personal information. The bill redefines "personal information" to include any information relating to an individual that can identify that individual, regardless of whether the information is encrypted.

SB 859 also adopts a new category of "private information" for which duties are imposed which includes social security numbers, driver's license or state identification card numbers, passport numbers, or other federally issued identification numbers and financial account numbers. The bill also defines fairly specific written data security procedures and practices that businesses must require from third-party contractors who handle personal information. If passed, SB 859 will impose new and expanded duties on nearly any business that keeps data regarding individual customers. SB 859 has been referred to the Senate Rules committee, but no hearing has been scheduled yet. SB 859 was cross-filed with HB 960, which is scheduled for a hearing in the House Economic Matters committee on February 20th.

SB 591 Governmental Procedures – Protection of Personal Information

SB 591 establishes rules for Maryland government agencies that are analogous to those currently applicable to private businesses under PIPA. The bill establishes rules regarding keeping, securing, and destroying records that contain personal information on Maryland residents and the response and notification duties in the event of a data breach. It would also require agencies that disclose personal information to third-party contractors to require that the contractors implement and maintain reasonable security procedures and practices, although it fails to define what "reasonable" practices will involve.

SB 591 narrowly defines "personal information" to include a resident's first name or first initial and last name in combination with any one or more of: (i) a social security number; (ii) a driver's license number; (iii) a financial account number; or (iv) a taxpayer identification number. "Personal information" is further limited by excluding encrypted information, and the bill adopts a broad definition of "encrypted" without reference to industry standards. SB 591 has been referred to the Senate Education, Health, and Environmental Affairs committee, and no hearing is scheduled as of the date of this alert.

SB 676 Governmental Procedures – Security and Protection of Information

SB 676 is a more expansive alternative to SB 591 which corresponds to the proposed revisions to PIPA under SB 859. SB 676 adopts definitions of "personal information," "private information," and "reasonable security procedures and practices" that are similar to the definitions in SB 859. SB 676 establishes broader duties for government agencies and provides greater protections to individuals than SB 591. SB 676 also creates new contractual requirements for private contractors who receive personal information from government agencies. A hearing on SB 676 in the Senate Education, Health, and Environmental Affairs committee is scheduled for February 21st. SB 859 was cross-filed with HB 959, which is scheduled for a hearing in the House Health and Government Operations committee on February 20th.

SB 624 Identity Fraud – Medical Records

SB 624 expands the crime of Identity Fraud to include accessing medical information or services. The bill prohibits: (i) knowingly, willfully, and with fraudulent intent possessing, obtaining, or helping another to possess or obtain personal identifying information to access medical information or services; (ii) knowingly and willfully assuming the identity of another to access medical information or services; and (iii) knowingly, willfully, and with fraudulent intent accessing medical information or services, skimming personal identifying information from the magnetic strip of a credit card, or re-encoding the magnetic strip of a credit card onto another card, in either case without the consent of the cardholder.

SB 624 also expands the definition of "personal identifying information" as it relates to identity fraud to include health insurance identification numbers, medical identification numbers, unique biometric data, and digital signatures. The bill considers the value of medical information or services in determining the maximum penalties available and allows for restitution orders to include the reasonable costs incurred to clear the victim's medical history or records. A hearing on SB 624 in the Senate Judicial Proceedings committee is scheduled for February 27th. SB 624 was cross-filed with HB 942, which is scheduled for a hearing in the House Judiciary committee on March 12th.

Venable LLP offers a broad array of legal services to a variety of different players within the cybersecurity arena. Our attorneys are adept at understanding complex client issues and tapping into the extensive experience of our many practice areas including privacy and data security, e-commerce, intellectual property, government contracting, and legislative and government affairs.

If you have any questions concerning this alert, please contact any of the authors.