



**E-COMMERCE, PRIVACY,
AND MARKETING
ATTORNEYS**

Two of the “Top 25 Privacy Experts”
by *Computerworld*

“Winning particular plaudits” for
“sophisticated enforcement work” –
Chambers and Partners

Authors/editors of the forthcoming
BNA Portfolio on Privacy Law

Recognized in the 2008 United
States editions of *Chambers USA*
and *Legal 500* for its outstanding
data protection and privacy practice

“Among the nation’s first privacy
lawyers” – *Chambers and Partners*

**EDITORS AND
CONTRIBUTORS**

Emilio W. Cividanes
ecividanes@venable.com
202.344.4414

Stuart P. Ingis
singis@venable.com
202.344.4613

Michael A. Signorelli
masignorelli@venable.com
202.344.8050

Tara M. Sugiyama
tmsugiyama@venable.com
202.344.4363

1.888.VENABLE
www.Venable.com

In this Issue:

Heard on the Hill:

- Senate Commerce Committee Investigates ISP Based Advertising

New Online Safety Laws:

- PROTECT Our Children Act
- KIDS Act
- Protecting Children in the 21st Century Act
- Identity Theft Enforcement Act/Cybercrime Act
- Ryan Haight Online Pharmacy Act

Around the Agencies:

- Proposed Labeling Requirements for Advertisements Depicting Toys and Games
- FTC v. Patten

From the States:

- Nevada’s Encryption Law Becomes Effective
- Massachusetts Passes New Data Security Regulations

Congress recessed following the passage of the financial bailout and headed home in preparation for the elections. Prior to recessing, Congress passed a flurry of Internet related legislation on issues that had been under consideration through the last several Congresses. The primary focus of the new legislation is online child protection.

This issue of the *Download* includes articles on the final Congressional hearing of the 110th Congress on Internet advertising, the key provisions of five new Internet related laws, a new proposed rulemaking that would impose labeling requirements on advertisements for toys and games, and a recent enforcement action brought by the Federal Trade Commission. Finally, there are two articles describing new data security requirements in Nevada and Massachusetts.

Senate Commerce Committee Investigates ISP Based Advertising

Congress held several hearings this session investigating the impact of online advertising practices on consumer privacy. On September 25, 2008, the Senate Commerce Committee held the last hearing of the 110th Congress on this issue. Specifically, the Committee examined the impact broadband access providers' advertising practices have on consumer privacy and considered whether legislation or self-regulation is required to address privacy concerns associated with online behavioral advertising.

I. Congressional Opinion

There was a general consensus among Committee members that a more comprehensive understanding of online behavioral advertising was necessary before introducing legislation. Sen. Dorgan (D-ND) stated that it was premature to determine whether self-regulation with enforcement capabilities or legislation presents the best solution to address privacy concerns. Sen. Hutchison (R-TX) cautioned against legislating in the area of online behavioral advertising before gaining a better understanding of the evolving technology, stating that innovation should not be hindered. She also stated that greater transparency and disclosure are important. Sen. Vitter (R-LA) indicated that any approach should not be technology-specific. Senators Thune (R-SD) and Wicker (R-MS) supported the development of comprehensive self-regulatory guidelines to govern online behavioral advertising.

II. Industry Supports Self-Regulation

AT&T and Time Warner Cable appeared before the Committee indicating that they did not engage in online behavioral advertising. Verizon Communications specified that it does not use deep packet inspection to target advertising to consumers, but rather that its online advertising practices are based on other technologies, such as the use of cookies or ad delivery servers to provide advertising that is limited to Verizon's own services or web sites. All three witnesses expressed support for a self-regulatory framework for online behavioral advertising that incorporates affirmative opt-in consent, consumer control, transparency, privacy protection, and consumer value. Verizon also stated it supports a best practices framework that includes a certification process for companies demonstrating adherence to their collection and use of information for online behavioral advertising practices. Although Verizon opposed legislation, Verizon expressed support for providing the Federal Trade Commission with authority to take measures against companies failing to comply with a self-regulatory framework.

The three witnesses encouraged all participants in online advertising, including ad networks, publishers, search engines, ISPs, browser developers, and other application providers, to commit to a self-regulatory framework.

III. Witness Calls for Legislation

Public Knowledge (“PK”) expressed support for comprehensive legislation covering the entire Internet ecosystem to address privacy concerns that arise in the online behavioral advertising arena. PK said that consumers rather than the ISPs should have the option to decide what information is sensitive. In addition, PK raised concerns regarding the use of certain technologies employed for advertising purposes.

NEW ONLINE SAFETY LAWS

PROTECT Our Children Act

PROTECT Our Children Act, introduced by Sen. Biden (D-DE), was signed into law by the President on October 13, 2008. The Act modifies the federal criminal code to extend new reporting requirements to providers of “electronic communication services” or “remote computing services” (“Providers”) with “actual knowledge” of incidents involving child pornography.¹ Providers would be required to report such incidents to the National Center for Missing and Exploited Children (“NCMEC”) and CyberTipline. By amending the criminal code, the Act subjects Providers to the types of reporting and data retention obligations imposed on Internet service providers. While the Act requires a Provider to make a report when it obtains “actual knowledge,” the Act expressly indicates that it would not require Providers to monitor its users, subscribers, or customers; monitor the content of any communication of any person; or affirmatively seek facts or circumstances related to a reportable incident.²

Below is a summary of the Act’s reporting and retention requirements and the enforcement and limited liability provisions.

I. Reporting Requirements – Sec. 2258A(b)(1-5)

The Act requires Providers to report to NCMEC certain information related to apparent child pornography, the individual involved, and the circumstances surrounding the images. Set forth below is specific information that are required to be included in a report to NCMEC:

- Information about the Involved Individual—identity of any individual who appears to have violated the law (i.e. email address, IP address, URL, or any other identifying information, including self-reported identifying information).
- Historical Reference—information related to when and how the individual uploaded, transmitted, or received the material or how the provider obtained “actual knowledge” of the apparent child pornography (i.e. reported to, or discovered by the provider). Information should include a date and time stamp and time zone.
- Geographic Location Information—information relating to the geographic location of the involved individual or website (e.g. IP address, verified billing address, or at least one form of geographic identifying information, including area code or zip code, and any self-reported geographic identifying information).
- Images of Apparent Child Pornography—any image of the apparent child pornography that is the subject of the report.

¹ S. 1738, Sec. 501 amendment Sec. 2258A(a)(1).

² Sec. 2258A(f).

- Complete Communication for the Image—the image should be accompanied by any data or information regarding the transmission of the communication and any images, data, or other digital files in, or attached to, the communication.

II. Retention Requirements – Sec. 2258A(h)(1-5)

A Provider is required to preserve the contents of the report for 90 days from the date it receives notification by the CyberTipline receipt of the report. The Act requires Providers to preserve any images, data, or other digital files commingled or dispersed among the images of apparent child pornography within a particular communication or user created folder or directory. The Act also requires Providers to preserve material in a secure location and to limit access to the material.

III. Enforcement & Limited Liability – Sec. 2258A(e) and Sec. 2258B

Any Provider that knowingly and willfully fails to make a report to NCMEC could be fined up to \$150,000. For any subsequent failure to report, the Provider could be fined up to \$300,000.

The Act specifically exempts electronic communications service providers, remote computer service providers, and domain name registrars from civil claim or criminal charge arising from the performance of the reporting requirements under the Act, provided such entities do not engage in intentional misconduct or reckless behavior. The Act also requires such entities to minimize the number of employees having access to any image depicting child pornography and to permanently destroy such images upon notification from law enforcement.

KIDS Act

The “Keeping the Internet Devoid of Sexual Predators Act” or the “KIDS Act,” introduced by Sen. Schumer (D-NY), was signed by the President on October 13, 2008. The new law requires convicted sex offenders to register Internet identifiers in the National Sex Offender Registry. Additionally, the Act grants the Attorney General authority to permit social networking websites to cross-check their databases with the online identifiers in the registry on a voluntary basis. Below is a summary of the Act.

I. Direction to the Attorney General, Sec. 2

The Act mandates the Attorney General to require sex offenders to provide the National Sex Offender Registry with “Internet identifiers” that sex offenders use. “Internet identifiers” are email addresses and “other designations used for self identification or routing in Internet communication or posting.” The Act also provides the Attorney General with the authority to specify the time and manner by which sex offenders must keep the information they provide to the registry current. The Act prohibits the disclosure of the sex offender’s Internet identifiers to the general public. Additionally, the Act requires the Attorney General to ensure that procedures exist to notify sex offenders of any requirement changes under the new law.

II. Checking System for Social Networking Websites, Sec. 3

a. Secure System for Comparisons—

The Act requires the Attorney General to establish and maintain a secure system allowing social networking websites to compare information contained in the registry with Internet identifiers of its users. Under the provisions of the Act, if a social networking website receives a matched Internet identifier, the Attorney General must provide information relating to the identity of the individual upon request. The Act limits this information to the following: name, sex, resident address, photograph, and physical description. Additionally, the Act limits the release of Internet identifiers; specifically, that the Attorney General and social networking websites may not release to the public any list of Internet identifiers of the sex offenders in the system.

b. Access to & Use of System—

A social networking website seeking to use the secure system must submit an application and pay the fee requirement to the Attorney General in order to access the secure system. The Attorney General may deny, suspend, or terminate use of the secure system by a social networking website if the site: (1) provides false information in its application; (2) may be using the system for unlawful or improper purposes; (3) fails to comply with stated policies and procedures pertaining to individuals who are denied access to the site; or (4) uses information from the system in a manner that is inconsistent with the purposes of the law.

c. Limitation on Liability—

The Act prohibits the bringing of civil claims against social networking websites arising from the use by the website of the registry National Sex Offender Registry. The limitation on liability does not apply if a website has engaged in actual malice, intentional misconduct, or reckless disregard to a substantial risk of causing injury without legal justification. Social networking websites are also required to minimize the number of employees provided access to the Internet identifiers for which a match has been found on the system.

III. Modification of Minimum Standards Required for Electronic Monitoring Units Used in Sexual Offender Monitoring Pilot Program, Sec. 4

Section 4 of the Act amends the Adam Walsh Child Protection and Safety Act revising the minimum standards for electronic monitoring of sex offenders under a pilot program by eliminating the requirements that a tracking device contain cellular technology and provide two- and three-way voice communication.

The Protecting Children in the 21st Century Act

On October 10, 2008, the President signed into law the “Protecting Children in the 21st Century Act.” The stated aim of the law is to promote a safe Internet for children and to enhance child pornography enforcement. Among the provisions of the law, the Act mandates the Federal Trade Commission (FTC) to carry out a public awareness campaign to promote the safe use of the Internet by children. The law also establishes a working group to examine online safety for children. Additionally, the law requires

certain schools to certify that their Internet safety policies educate minors about appropriate online behavior. Set forth below are the key provisions of the Act.

I. Promoting a Safe Internet for Children

a. Carrying out a Public Awareness Campaign

The Protecting Children in the 21st Century Act mandates the FTC to carry out a public awareness campaign to educate the public about methods to promote the safe use of the Internet by children. The FTC is directed to use existing governmental resources as well as resources of nonprofits, private technology and financial companies, and Internet service providers to carry out the public awareness campaign. This campaign includes identifying and promoting best practices for Internet safety, establishing and carrying out a national outreach and education campaign pertaining to Internet safety, promoting up-to-date knowledge of current issues, and facilitating access to Internet safety education and public awareness efforts by state and local governments, schools, police departments, and nonprofits.

b. Establishing an Online Safety and Technology Working Group

The new law requires the Assistant Secretary of Commerce for Communications and Information to establish an Online Safety and Technology working group. This group will include representatives of the business community, public interest groups, and other appropriate groups and Federal agencies. The working group is required to evaluate the status of industry efforts to promote online safety through educational efforts, parental control technology, filtering software, labeling, and other technologies. The group will also examine the status of industry efforts to promote online safety among providers of electronic communications services and remote computing services. The law further calls on the group to evaluate the practices of electronic communications service providers and remote computing service providers pertaining to record retention of crimes against children. Furthermore, the law calls for an evaluation of the development of technologies to assist parents protect children from inappropriate material online.

c. Promoting Online Safety in Schools

In the context of promoting online safety in schools, the law requires that as part of its Internet safety policy, a school, school board, local educational agency, or other authority must certify that the school educates minors about appropriate online behaviors; such as interacting with others on social networking websites and in chat rooms, and cyberbullying awareness and response.

II. Enhanced Child Pornography Enforcement

Lastly, the law enhances child pornography enforcement by making any person who violates any provision of section 2252 of Title 18, which addresses certain activities relating to material involving the sexual exploitation of minors, liable to the United States for a forfeiture penalty.

Identity Theft Enforcement and Restitution Act

The “Identity Theft Enforcement and Restitution Act” became law on September 26, 2008. The Act does not include the data security breach requirements proposed in other related legislation. However, the Act does provide the Department of Justice with new tools to combat identity theft and cyber-crime. In particular, the law imposes criminal liability on bad actors while not regulating technology. This law also incorporates recommendations from the President’s Identity Theft Task Force.

Of specific note in the “spyware” debate, this Act provides law enforcement with broader ability to combat bad actors. Section 204 of the Act amends the Computer Fraud and Abuse Act (“CFAA”) to address the malicious use of spyware to steal sensitive personal information. Specifically, the Act eliminates the requirement that the loss resulting from the damage to a victim’s computer must exceed \$5,000. Eliminating the financial threshold should aid law enforcement efforts and increase prosecutions.

The Act creates new criminal offenses involving attacks on multiple computers, by making it a felony to employ spyware or keyloggers to damage 10 or more computers, regardless of the aggregate amount of damage caused. Removing this threshold requirement should aid law enforcement by ensuring that the most egregious identity thieves will not escape with a minimal, or no, sentence. Violators of the provision who knowingly transmit a program that intentionally causes damage without authorization to 10 or more computers would be subject to a criminal fine, or imprisonment for not more than 10 years, or both. Violators who intentionally access 10 or more computers without authorization and recklessly cause damage are subject to a criminal fine, or imprisonment for not more than 5 years, or both.

In addition to the above instances involving damage to 10 or more computers, the law imposes a punishment of a fine, imprisonment of not more than 5 years, or both, in circumstances where protected computers are intentionally accessed without authorization, and results in reckless damage. If, instead of “recklessly causing damage,” the intentional access “causes damage and loss,” the Act increases the punishment to a fine, or imprisonment of not more than 10 years, or both. This 10 year punishment also applies if an offender knowingly causes the transmission of a program that results in any of the above 5 harms (or damage to 10 or more computers).

The Ryan Haight Online Pharmacy Consumer Protection Act of 2008

On October 15, 2008, the “Ryan Haight Online Pharmacy Consumer Protection Act of 2008” (the “Act”) was signed by the President and became law. The Act amends the Controlled Substances Act to address online pharmacies and requires at least one in-person medical evaluation of a patient for a prescription to be valid. Additionally, the Act imposes registration and reporting requirements on online pharmacies.

I. Valid Prescription Requires In-Person Medical Evaluation

The Act amends the Controlled Substances Act to address controlled substances dispensed over the Internet. Specifically, the delivery, distribution, or dispensing of controlled substances over the Internet without a valid prescription is prohibited. A prescription is valid only when issued for a legitimate medical purpose and by a practitioner who has conducted a minimum of one in-person medical evaluation of the patient or by a covering practitioner. This requirement does not apply to telemedicine practitioners.

II. Online Pharmacy Registration Requirements

Additionally, the Act imposes registration requirements on online pharmacies. For those pharmacies registered to dispense or conduct research with controlled substances, the Attorney General has the authority to extend the scope of those registrations to cover the dispensing of controlled substances over the Internet. The Attorney General has the option to deny any registration request that would be inconsistent with the public interest.

III. Reporting, Disclosure & Licensing Requirements for Online Pharmacies

For those pharmacies with modified registrations permitting them to dispense controlled substances over the Internet, the Act imposes reporting requirements on them. Specifically, the Act requires such pharmacies to report to the Attorney General the controlled substances they dispense, in the amount specified, and in the time and manner specified by the Attorney General. This reporting requirement applies only once a pharmacy meets specified monthly thresholds.

The Act requires an online pharmacy’s homepage to display in a visible and clear manner, a statement that the pharmacy complies with the requirements of the Act regarding the delivery, sale, or offer for sale of controlled substances. In addition, the homepage is required to display a declaration that they are acting in accordance with the Act.

Furthermore, the Act requires online pharmacies to comply with state laws governing licensure of pharmacies in each state from which and to which they deliver, distribute, or dispense, or offer to deliver, distribute, or dispense, controlled substances over the Internet.

IV. Criminal Penalties and Offenses

The Act increases criminal penalties involving controlled substances in Schedules III, IV, and V of the Controlled Substances Act. Additionally the Act amends the Controlled Substances Act by stating that it is unlawful for any person to knowingly or intentionally deliver, distribute, or dispense (or aid or abet in the delivery, distribution, or dispensing of) a controlled substance over the Internet in an unauthorized manner. The Act further states it is unlawful to knowingly or intentionally use the Internet, or cause it to be used, to advertise the sale of or offer to sell, distribute, or dispense a controlled substance in an unauthorized manner.

V. State Cause of Action

Although the Act provides for no private right of action, the Act provides the Attorney General of any state with the authority to bring a civil action in a district court. Such actions would be to enjoin conduct that violates the Act, to enforce compliance with the Act, to obtain damages, restitution, or other compensation, or to obtain other appropriate legal or equitable relief in any case where a state has reason to believe the interests of its residents have been adversely affected by actions violating the Act.

AROUND THE AGENCIES

Proposed Labeling Requirements for Advertisements Depicting Toys and Games

The Consumer Product Safety Commission (“Commission”) issued proposed rules for comment related to advertising for certain toys and games in catalogues and other printed materials, including Internet advertising.³ The proposal is a result of the Consumer Protection Safety Improvement Act (“Act”) passed in August 2008. The Act requires specific labeling on advertisements for toys and games that are intended for use by children between 3 to 6 years old and that contain small parts (e.g. balloons, small balls, or marbles) that could pose a choking hazard. The proposed rules explicitly prescribe the content, size, and location of cautionary statements that would need to be included in advertisements.

The statute distinguishes between labeling for advertisements on the Internet and advertisements in catalogues and other printed materials. The statutory obligation related to Internet advertising becomes effective December 12, 2008. The Commission has proposed delaying the effective date for catalogue and other print materials from February 10, 2009 until August 9, 2009. Comments on the requirements imposed on catalogues and other print materials were due October 20, 2008 and comments concerning Internet advertising are due November 20, 2008. Below is a summary of the proposed rules and specific topics for which the Commission seeks comment.

³ Labeling Requirement for Toy and Game Advertisements, 73 Fed. Reg. 58063 (Oct. 6, 2008).

I. Guidelines for Cautionary Statements

The Act imposes labeling requirements for advertising of products that could pose a choking hazard. Specifically, the Act requires that cautionary statements must be displayed conspicuously and in a legible type that contrast by typography, layout, or color with other material printed or displayed in the advertisement. The proposed rules also specify the content, size, and placement requirements for cautionary statements. In addition, the proposed rules require that the cautionary statement be provided in same language used in the advertisement.

A. Catalogue and Other Printed Material Rules

The Commission's proposed rule prescribes the content and type-size of cautionary statements that are required for advertisements in catalogues and other printed materials. The type-size requirements are based on the size of the advertisements for the specific toy or game. Specifically, the proposed rule applies the minimum type size and other requirements imposed on product labeling. These requirements are based on the federal regulations located in 16 C.F.R. 1500.121, which impose very specific type-size, location, and other labeling requirements. The proposed rules, however, would require that labeling statements could not be smaller than 0.08 inches, and all labeling statements must be printed in type that is not smaller than the largest of any other statements or text, other than the product or article name, in the advertisement.

The proposed rule would permit the use of shorthand, or abbreviated warnings for catalogues and other printed materials where it is difficult to include full cautionary statements because of the size of the advertisement. The rules would require that the shorthand terms (e.g. "SMALL PARTS. Not for < 3 yrs," which means "Small Parts. Not for children under 3 yrs.") be defined with full warnings at the bottom or top of each page of the catalogue. In the alternative, the terms could be defined across two facing pages of both pages that contain products to which the warning applies.

B. Internet Warnings

The Commission has also proposed rules with respect to requirements for Internet advertising. Similar to the proposed rule's requirement for advertisements in catalogues and other printed materials, the Commission has proposed to also apply the requirements found in 16 C.F.R. 1500.121 to cautionary statements included in Internet advertisements. The Commission, however, indicated that the size of Internet advertisements makes it difficult to readily adopt the minimum type-size requirements found in 16 C.F.R. 1500.121. The Commission, therefore, proposed a rule that would require that all labeling statements be printed in type that is no smaller than the largest of any other statements or text, other than the product or article name, in the advertisement. In addition, the rule would require any cautionary statement be located immediately before any other statements or text in the advertisement that describes the function, use, or characteristics of the article being advertised. The Commission indicated that it proposed this rule to address concerns that statements may be located below the page scroll of a web site. The Commission also made a preliminary finding that the use of abbreviated warnings in the place of full text warnings is unnecessary and undesirable in the context of Internet advertising.

II. Request for Comments

The Commission has asked for interested parties to comment on the following specific issues:

1. The abbreviated versions and the minimum type-size and placement requirements of the cautionary statements as proposed in the rule;
2. The impact on businesses from the proposals on minimum type-size and placement in catalogues and other printed materials;
3. How often catalogues or other written materials are published and how much lead time is required to prepare these materials for publication;
4. The cost of publishing new catalogues to meet these requirements without the 180 day grace period; and
5. Whether the advertising requirements for catalogues and other printed materials should also apply to materials distributed solely between businesses and not to ultimate consumers, and, if not, how the Commission can distinguish catalogues distributed solely between businesses from those intended for final distribution to ultimate consumers, which may include institutions such as schools, churches, day care centers, and recreational facilities.⁴

Telemarketing Sales Rule Violations

The Federal Trade Commission (FTC) on October 1, 2008, reached a settlement with list broker Glenn L. Patten and two companies he operates (“Patten”). The FTC alleged that Patten, both individually and doing business as Glenn L. Patten Marketing Solutions and Marketing Solutions, engaged in deceptive acts in violation of the FTC Act and the Telemarketing Sales Rule. Patten allegedly sold or rented “full data leads” to telemarketers, without obtaining prior consent from consumers, when Patten knew or consciously avoided knowing that the telemarketers were promoting advance fee credit products. The “full data leads” included consumers’: (1) bank account and routing information, (2) credit card numbers, (3) credit card security codes, and (4) credit card expiration dates. Additionally, Patten allegedly provided telemarketers with unencrypted consumer account numbers (e.g. credit or debit card numbers, bank account numbers, and PINs,) in violation of the TSR.

If the settlement is approved by U.S. District Court for the Northern District of Illinois, Eastern Division, Patten will be prohibited from directly (or assisting others in) collecting, selling, renting, brokering, purchasing, transferring, or otherwise disclosing consumers’ account numbers, to, from, for, or with any unaffiliated third party for marketing purposes. This prohibition, however, does not prevent Patten from collecting the account

⁴ 73 Fed. Reg. at 58066.

and disclosing numbers of his own customers for the purpose of completing authorized transactions. Additionally, the order requires Patten to:

- turn over to the FTC all his lists of consumers' account numbers;
- monitor the advertising and promotional materials and activities of his clients to determine the nature of products or services sold to consumers;
- investigate any complaint or refund request regarding the practices of Patten's clients;
- terminate services to any person whom he knows or should know is engaging in misrepresentations to any consumer's decision pertaining to offered transactions or the billing of accounts without consumer authorization; and
- provide the FTC with all relevant information of any person to whom Patten terminates services.

FROM THE STATES

Nevada's Encryption Law Becomes Effective

The encryption provision of Nevada's breach notification law, which was enacted over three years ago, became effective on October 1, 2008. This section requires businesses in Nevada to encrypt customer "personal information" before electronically transmitting such information outside the "secure system of the business." This provision, however, does not apply to fax transmissions. Businesses in Nevada thus must now be aware that the electronic transmission of unencrypted customer "personal information" outside of a business's secure systems may constitute a violation of Nevada's data security law. Below is a summary of the key sections of the law.

I. Background

Nevada's security breach law was signed by the governor on June 17, 2005, and the security breach notification and other identity theft provisions of the law were effective by January 1, 2006. The effective date of the encryption provision of the law was delayed to provide Nevada businesses with sufficient time to implement new encryption software.

II. Personal Information

Nevada law requires a business to encrypt "personal information" before it may electronically transfer such information outside of the "secure system of the business." Under Nevada law "personal information" includes a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (1) Social Security number or employer identification number; (2) driver's license number or identification card number; (3) account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account.

III. Encryption Requirements

Nevada law directs businesses to use any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding, or a computer contaminant, to: (1) prevent, impede, delay or disrupt access to

any data, information, image, program, signal, or sound; (2) cause or make any data, information, image, program, signal, or sound unintelligible or unusable; or (3) prevent, impede, delay or disrupt the normal operation or use of any component, device, equipment, system, or network.

Massachusetts Passes New Data Security Regulations

On September 19, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation issued a set of final regulations establishing standards for how businesses must protect and store personal information of Massachusetts consumers. Among the key requirements, businesses must now encrypt all personal information of Massachusetts residents transmitted across public networks or wirelessly, and such information that is stored on laptops or other portable devices. These regulations, designated in 201 Mass. Code Regs. 17.00 et seq., are not set to take effect until January 1, 2009.

The new regulations apply to all businesses and individuals that own, license, store, or maintain personal information of Massachusetts residents. The stated purpose of the regulations is to establish minimum standards that these businesses and individuals must meet to safeguard personal information contained in both paper and electronic records.

I. Comprehensive Security Program

The regulations impose a duty on covered businesses and individuals to develop, implement, maintain, and monitor a comprehensive, written information security program that applies to any “records” containing personal information of Massachusetts residents. As defined in the regulations, “records” means “any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.” The regulations further state that the program must be consistent with industry standards, and contain administrative, technical, and physical safeguards to ensure the security and confidentiality of the records.

To determine whether a security program complies with the regulations, the following factors are considered: (1) the size, scope, and type of business; (2) the resources available to the business; (3) the amount of stored data; and (4) the need for security and confidentiality of the information.

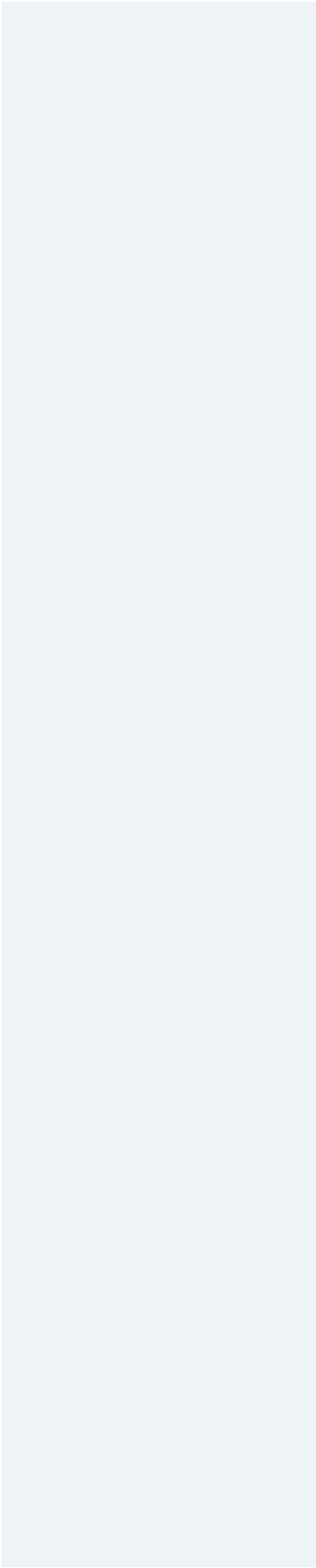
As outlined in the regulations, every comprehensive security program must, at a minimum, include the following:

- Designation of one or more employees to maintain the security program;
- Identification and assessment of internal and external risks to the security, confidentiality, and/or integrity of any records containing personal information, and an evaluation of the effectiveness of current safeguards to limit these risks, including:
 - ~ Ongoing employee training,
 - ~ Employee compliance, and
 - ~ Means for detecting and preventing security system failures;

- Development of security policies for employees addressing whether and how employees should keep, access, and transport records with personal information outside the business' premises;
- Establishment of disciplinary measures for violation of program rules;
- Prevention of terminated employees from accessing records with personal information by immediately terminating their physical and electronic access to the records;
- Verification that third-party service providers with access to the personal information have the ability to protect the information, and such providers are bound by contract to maintain the safeguards;
- Receipt of written certification that a third-party service provider with access to personal information is in compliance with the regulations;
- Limitation on amount of personal information collected and its retention, and the restriction of access such information to a need-to-know basis;
- Identification of records, computing systems, and storage media to determine which records contain personal information;
- Restrictions on physical access to and storage of records containing personal information;
- Regular monitoring of employee access to personal information;
- Review of scope of security measures annually or when material changes take place in business practices; and
- Documentation of responsive actions taken regarding security breach incidents and a mandatory post-incident review to change business practices pertaining to the protection of personal information.

II. Electronic Record Security Requirements Including Mandatory Encryption

For those businesses and individuals that own, license, store, or maintain personal information on Massachusetts residents and electronically store or transmit such personal information, the regulations also require them to establish and maintain security systems that cover computers, including wireless systems, as part of the above comprehensive information security programs. Perhaps most pressing for businesses, is that these computer security systems must now include the following two features: (1) encryption of all transmitted records and files that will travel across public networks and encryption of all data transmitted wirelessly; and (2) encryption of all personal information on laptops and other portable devices.



Additional requirements for the computer security systems include:

- (1) secure use authentication protocols;
- (2) secure access control measures;
- (3) monitoring of systems for unauthorized use of or access to personal information;
- (4) current firewall protection and operating system security patches for files containing personal information on systems connected to the Internet;
- (5) current versions of system security agent software that includes malware protection, current patches, and virus definitions, or software that can be supported with current patches and virus definitions and is programmed regularly to receive current security updates; and
- (6) education and training for employees on why personal information security is importance and how to use the computer security system.

About Venable

One of *American Lawyer's* top 100 law firms, Venable LLP has attorneys practicing in all areas of corporate and business law, complex litigation, intellectual property and government affairs. Venable serves corporate, institutional, governmental, nonprofit and individual clients throughout the U.S. and around the world from its headquarters in Washington, D.C. and offices in California, Maryland, New York, and Virginia.

Venable office locations

BALTIMORE, MD

750 E. PRATT STREET
NINTH FLOOR
BALTIMORE, MD 21202
t 410.244.7400
f 410.244.7742

ROCKVILLE, MD

ONE CHURCH STREET
FIFTH FLOOR
ROCKVILLE, MD 20850
t 301.217.5600
f 301.217.5617

WASHINGTON, DC

575 SEVENTH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300

LOS ANGELES, CA

2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
t 310.229.9900
f 310.229.9901

TOWSON, MD

210 ALLEGHENY AVENUE
TOWSON, MD 21204
t 410.494.6200
f 410.821.0147

NEW YORK, NY

ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
TWENTY-FIFTH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

TYSONS CORNER, VA

8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
t 703.760.1600
f 703.821.8949

The *Download* is published by the law firm of Venable LLP. It is not intended to provide legal advice or opinion. Such advice may only be given when related to specific fact situations. You're receiving this communication because you are valued client or friend of Venable LLP. Questions and comments concerning information in this newsletter should be directed to Stuart Ingis at singis@venable.com