

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY

PREPARED BY
FOLEY & LARDNER LLP AND EVERSHEDES LLP

NOVEMBER, 2009

©2009 Foley & Lardner LLP • Attorney Advertisement • Prior results do not guarantee a similar outcome • 321 North Clark Street, Chicago, IL 60654 • 312.832.4500 –
This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.



CONTACTS

Austria

Georg Roehsner

Tel: +43 15 16 20 16 0
g.roehsner@lamberteversheds.com

Belgium

Koen Devos

Tel: +32 2 737 9360
koendevos@eversheds.com

Czech Republic

Marek Bomba

Tel: +420 251 009 111
marek.bomba@bapol.cz

Denmark

Hans Juhler

Tel: +45 33 75 05 88
hansjuhler@eversheds.com

Estonia

Aleksandr Kostjuevits

Tel: +372 614 1990
aleksandr.kostjuevits@eversheds.ee

France

Marc Lempérière

Tel: +33 15 57 34 11 2
marclempérière@eversheds.com

Germany

Alexander Niethammer

Tel: +49 89 54 56 53 18
alexander.niethammer@eversheds.de

Middle East

Jennifer Westall

Tel: +974 496 7388
jenniferwestall@eversheds.com

Netherlands

Michel Chatelin (Amsterdam)

Tel: +31 10 24 88 03 5
michelchatelin@eversheds.nl

Poland

Arwid Mednis

Tel: +48 22 5050 766
arwid.mednis@wierzowski.pl

P R China

Peter Corne

Tel: +86 21 61 37 10 01
petercorne@eversheds.com

Singapore

Sze-Hui Goh

Tel: +65 9762 7322
sze-huigoh@eversheds.com

Slovakia

Nada Loviskova

Tel: + 421 220 251 311
nada.loviskova@bapol.cz

South Africa

Bradley Scop

Tel: +27 11 52 36 094
bradleyscop@eversheds.co.za

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

Hong Kong

Michael Yau

Tel: +85 22 71 88 937
michaelyau@eversheds.com

Hungary

Agnes Szent-Ivany

Tel: +36 1 394 3121
szent-ivany@sandor-advocat.hu

Ireland

David Fagan

Tel: +35 31 66 44 27 3
dfagan@eversheds.ie

Italy

Andrea Zincone

Tel: +39 06 32 25 84 4
andreazincone@eversheds.it

Japan

Etsuo Doi

edoi@foley.com

Masa Tanabe

mtanabe@foley.com

Lithuania

Jonas Saladzius

Tel:+370 5 239 2362
jonas.saladzius@evershedssaladzius.lt

Spain

Jesús Diaz-Mauriño Garrido-Lestache

Tel: +34 91 436 00 90
jdm@evershedslupicinio.com

Sweden

Anders Larsson

Tel: +46 85 45 32 20 0
anderslarsson@eversheds.se

Switzerland

Claudius Triebold and Monika Quillen

Tel: +41 44 20 49 09 0
claudius.triebold@eversheds.ch

United Kingdom

Paula Barrett

Tel: +44 161 831 4890
paulabarrett@eversheds.com

United States

Andrew Serwin (San Diego, California)

Tel: +1 619 685 6428
aserwin@foley.com

Peter McLaughlin (Boston, Massachusetts)

Tel: +1 617 502 3265
pmclaughlin@foley.com

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY

(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Austria Austrian Data Protection Act ("DSG")	There is no explicit rule in the DSG requiring the regulator or individuals to be notified. Notification requirements can only be deducted from the general rules and principles of Austrian civil law. Therefore notification requirements can result out of a contractual relation and/or binding corporate rules or as an expression of the general principles of civil law, according to which, each party has to act in good faith.	None prescribed Due to general regulations in the Austrian civil law, measures have to be taken in the most expedient manner in order to limit damages	None prescribed	§ 11 DSG contains several duties for the processor, e.g. to use data only according to the instructions of the controller, to take all required safety measures, to create in agreement with the controller the necessary technical and organizational requirements for the fulfillment of the controller's obligation to grant the right of information, rectification and erasure; to make available to the controller all information	N/A	N/A	Compensation for damages will only be admitted according to the general principles of Austrian civil law.	No

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>§ 24 DSG postulates that Information shall be given to the data subjects if this is necessary for fair and lawful processing, from which it might be argued that notification obligations could be drawn.</p> <p>A planned amendment of the DSG for 2010 introduces the new § 24 Abs 2a DSG according to which the data controller has to inform the person concerned immediately after getting awareness of a breach. But so far there is no</p>			<p>necessary to control the compliance with the obligations mentioned above. However, as mentioned at * there are no express reporting obligations.</p>				

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	certainty that the amendment will be implemented and if so, there are no exact specifications when and in what form the notification should happen.							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Belgium Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998	The applicable Belgian legislation does not include specific requirements to notify the individuals concerned or the regulator in case of a security breach. Therefore it is not mandatory, unless the requirement of notice is stipulated in contractual terms or binding corporate rules. However in the light of the general principles of civil law, a party always has to act in good faith. On the basis of the general principle of good faith and	None prescribed	None prescribed	No	N/A	N/A	Since the Law of December 8, 1992 does not stipulate mandatory rules concerning notice requirements in case of a security breach, no specific rules concerning damages or enforcement in case of a security breach are stipulated. Breach of the law can give rise to fines and claim for damages.	N/A

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	depending on the specific circumstances of the case, it could be appropriate to notify the individual in case of a security breach, certainly if this breach (and lack of notice of the breach) would cause damage to the individual concerned.							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
China	<p>There is currently no data protection legislation in force in China, although a draft privacy law was circulated for comments a number of years ago. There is therefore no statutory requirement to notify affected parties upon an information security breach.</p> <p>It is, however, possible to implement internal data protection processes on a contractual basis instead by incorporating measures</p>	None prescribed	None prescribed	No	N/A	N/A	None – see general comment	N/A

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>associated with international best practice into employee handbooks and tying compliance with such provisions to individual emp. contract performance. A breach of information security obligations set forth in employee handbooks would accordingly trigger a breach of employment contract and could lead to the ability of an employer to unilaterally terminate the same.</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
<p>Czech Republic</p> <p>Act No. 101 of April 4, 2000 on the Protection of Personal Data and on Amendments to Some Related Acts</p>	<p>Reporting is required. Whilst there is no express reporting requirement this requirement can be construed as necessary in order to satisfy one of the general principles imposed by the legislation, i.e. to protect each individual from unauthorized processing of its personal data. On that basis it is necessary to make a disclosure of the breach and notify each individual concerned.</p>	<p>No particular rules in place.</p> <p>However, in order to avoid any potential claims from affected individuals and in order to satisfy a general duty to act with due care, it is desirable to make an early disclosure of a breach.</p> <p>Also, early communication with the Data Protection Office is recommended.</p>	<p>There are no rules in place as regards form of disclosure notice. Practically any suitable tool of communication is sufficient (oral announcement to employees, publication on webpage for customers, contact by a telephone with recording of communication etc).</p>	<p>No particular rules are in place.</p> <p>Early disclosure/notification to the Data Protection Office is recommended.</p>	<p>There are no procedures prescribed by the law.</p> <p>It is recommended to act expeditiously and with maximum care.</p>	<p>No particular rules in place.</p>	<p>Damages can be sought by individuals concerned under the Civil Code, if the breach resulted in the violation of their "personality rights".</p> <p>Data Protection Office can impose financial penalties to a person administering personal data e.g. without consent of subjects/persons concerned.</p> <p>Violation of data protection laws can be also investigated and considered as a criminal offence –</p>	<p>N/A</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY

(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
							theft or unauthorized administration of personal data.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
<p>Denmark</p> <p>The Act on Processing of Personal Data (Act No. 429 of 31 May 2000)</p>	<p>While there are no specific rules on notification to the data subject / Data Protection Authorities (DPA) in relation to security breaches, DPA practice indicates an expectation of notice in some cases.</p> <p>The DPA does handle security breach cases if they become aware of any incidents. These cases provide the only guidelines on security breaches.</p> <p>The DPA's practice shows that notice</p>	<p>After the DPA has assessed the case they may require the controller to inform the affected individuals as soon as possible. Further to this the case assessment is published on the website of the DPA and the data maintaining entities may be required to take specific actions in respect of the data.</p>	<p>Depending on how personal the information is, the notice should be given to the affected individuals personally i.e. by sending a letter. If the case is serious, the notice should consist of as much information as possible.</p>	<p>None under the legislation. Check contractual obligations.</p>	<p>The controller can only use their own procedures if these are in accordance with the Danish Data Protection Act section 5 and section 41.3 and the policies set out by the DPA.</p>	<p>N/A</p>	<p>The Danish Data Protection Act does contain a penal provision in case of breach of section 5 and 41.3 of the Act. The penalty ranges from a fine up to 4 months of imprisonment. The data subject might bring an action for damages to the courts if certain criteria are fulfilled.</p>	<p>N/A</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	should be given to the individual affected after assessing the nature of the personal information and how many people are affected by the security breach. If the information is very personal and only few people are affected then notice should be given to each person individually							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
<p>Estonia</p> <p>Personal Data Protection Act of 12 February 2003</p>	<p>Both processors and controllers have security objectives under Estonia law. Both are referred to as processors, though the equivalent term for controller is 'chief processor'. Data processor must disclose information about a breach to the data subject on demand of the data subject.</p> <p>There is no express obligation to proactively notify of the breach.</p> <p>However, the data protection authority must be</p>	<p>Notification must be done within five working days after receipt of the data subjects' request.</p> <p>Notification to the data protection authority (if applicable) must be given immediately</p>	<p>Where possible the notification to the data subject must be given in the manner requested by the data subject.</p> <p>If the disclosure is required by the data protection authority the content of information and the way it shall be submitted is prescribed by the authority. It is possible to submit written notice or electronic notice (electronic signature required).</p>	<p>Yes. See notice column. After the breach is discovered the data processor must take measures to terminate the breach. If the breach related to sensitive personal data is not terminated, the responsible person (if appointed) must inform the data protection authority about the breach.</p>	<p>No.</p>	<p>It is possible to refuse to fulfill the request for notification of the data subject if notification may damage rights and freedoms of other persons, endanger the protection of the confidentiality of filiation of a child, hinder the prevention of a criminal offence or apprehension of a criminal offender, complicate the ascertainment of the truth in a criminal proceeding.</p>	<p>Violations of data protection requirements are treated as misdemeanors and are punishable by a fine.</p> <p>Civil enforcement actions may also be brought.</p>	<p>There is deemed compliance with the local law if the person complies with the relevant EC regulations.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	informed by responsible person (if appointed) if the data did not take measures to terminate the breach related to sensitive personal data. The data protection authority informs the data subject about the breach.							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY

(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
France	No duty to report the breach to the CNIL (French Data Protection Authority) or to the data subjects.			None.	No.		The breach of the data controller's obligation to ensure the security of the data is a criminal offence, which can be punished by up to 5 years of imprisonment and fines up to € 1,500,000 (for legal entities). In addition, the CNIL can pronounce fines up to € 300,000 and publicize the breach. Finally, the parties who suffer damages because of this breach can recover such damages from the courts.	No

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Germany	<p>Notice is required to concerned individuals as well as to the competent DP authority.</p> <p>Relevant data:</p> <ul style="list-style-type: none"> - sensitive personal data, - personal data falling under professional confidentiality requirements (medical records, client/attorney comm. etc.), - personal data relating to criminal or administrative offences or the suspect thereof, - personal data relating to bank or credit card 	At first, data recovery and protection measures must be taken. After that individuals must be informed without undue delay.	<p>Description of data security breach required; moreover, suggestions how to minimize the damage.</p> <p>The notice to authorities must, in addition, contain a description of the negative consequences and the rescue/ recovery measures taken.</p> <p>Form: as appropriate; in most cases notice in writing will be necessary.</p>	<p>The information duties must be fulfilled by the data controller (responsible addressee).</p> <p>The data processor must report data leaks or security breaches to the data controller.</p>	No.	Data not listed in column no. 1 is generally exempt.	<p>Administrative fines of up to 300.000 EUR are possible as well as criminal proceedings (up to 2 years imprisonment; further conditions apply).</p> <p>Non-notification where required is likely to qualify as an unfair trade practice which can be pursued by competitors or consumer protection societies.</p> <p>Civil liability is possible if the security measures taken by the data</p>	N/A

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>accounts.</p> <p>The data security breach must be able to cause "severe detriment" to the individual's rights.</p> <p>In case the efforts necessary to inform each person individually of the breach are inappropriate (e.g. because of the large no.), the information may be published in newspapers (further conditions apply).</p>						<p>controller were insufficient.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Hong Kong Personal Data (Privacy) Ordinance 1996	At present, there is no legal requirement for a data user to notify the regulator or individuals affected by personal data security breach or leakage. But the Hong Kong Government is considering the current position and may in the future introduce the notification requirements for personal data security breach notification	N/A	N/A	N/A	N/A	N/A	A data user shall take all practical steps to ensure that personal data held by it are protected against unauthorized or accidental access, processing, erasure or other use. If the leakage of personal data is caused by the data user's failure to comply with the above duty, it may be liable to the affected individuals for the damages caused.	N/A

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Hungary Act LXIII of 1992 on the protection of Personal Data and Public Access to Data of Public Interest	In Hungary there are no specific data protection rules regarding notice requirements in the case of a security breach. However, data controllers and data processors have underlying obligations to maintain the security and the protection of their data management procedures. Depending on the given case, these obligations might result in the obligation to notify individuals or authorities, considering also that data	N/A	N/A	No*	N/A	N/A	In the absence of mandatory rules on security breach notice, no damages are established by the law thereon. However, if the omission to notify results in the breach of general rules on security or civil law principles such as the obligation to cooperate or to mitigate damages, this might result in claims for damages. Please note that the breach of security regulations may result in criminal law liability as well.	No

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>controllers and data processors, like any other entity or person, have a general obligation under Civil law to cooperate in contractual relationships and to mitigate damages where applicable.</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Italy Legislative Decree No. 196 of June 30 2003	In Italy security breach notice is not strictly required, unless it is provided for by agreements, contracts and/or binding corporate rules in place in the concerned case. Failing any specific contractual provisions, however, in the light of the general principles of civil law requiring each party to act in good faith, it could be appropriate on a case by case evaluation to inform the other party, particularly when the lack of such information	N/A	N/A	No	N/A	N/A	As there are no express rules on reporting, there are no specific damages or enforcement linked to failure to report. However the breach itself may expose the controller to liability for fines and to claims for damages from the individuals affected.	No

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY

(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	could cause damage to said other party.							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Japan	<p>The Act on the Protection of Personal Information (the "Act") provides that the data collector must implement security safeguards necessary to prevent divulgence, loss or destruction of personal data (Article 20 of the Act), but it does not express any legal requirement to notify individuals or any governmental agencies.</p> <p>Some of the guidelines issued by various governmental agencies address</p>	Neither the Act nor the METI Guideline expresses the timing of Notice to Individual, Report to METI or Public Announcement.	<p>Neither the Act nor the METI Guideline expresses the form of Notice to Individual, Report to METI or Public Announcement.</p> <p>The METI Guideline describes the following two items as the purposes of Notice to Individual: (i) to apologize to the individual; and (ii) to prevent any secondary damages. Therefore, it can be speculated that the means and the contents thereof should be in accordance with these purposes.</p>	<p>The Act provides that the data collector must supervise the data processor so that they comply with Article 20 of the Act.</p> <p>The METI Guideline provides that such supervision includes: (i) entering into an appropriate service agreement with the data processor; and (ii) checking periodically whether the obligations under the service agreement are being followed. Furthermore, the</p>	<p>The Act does not express whether the data collector may use its own policies or procedures.</p> <p>The METI Guideline provides that necessary security safeguards would include adoption of certain security policies or procedures. Furthermore, the METI Guideline provides that it is "desirable" to include the following matters in such policies or procedures: (i) how to obtain and enter the data; (ii) how to transfer</p>	<p>The Act does not provide any exemption from Article 20 of the Act.</p> <p>The METI Guideline provides the following two criteria in order to be exempted from Notice to Individual: (i) there is no actual infringement of the individual's rights; and (ii) there is no, or only minimal, possibility of such infringement in the future. Furthermore, the METI Guideline lists the following three examples</p>	<p>The governmental agency in charge is entitled to recommend (<i>kankoku</i>) necessary measures to cease violation of Article 20 of the Act. If the data controller does not follow the recommendation, the governmental agency is entitled to order (<i>meirei</i>) implementation of such necessary measures.</p> <p>Any data controller that does not obey the above order is subject to imprisonment of 6 months or less, or a fine of 300,000</p>	No.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>this issue of notification. For example, the guideline issued by Ministry of Economy, Trade and Industry (the "METI Guideline") lists the following two examples as "desirable" countermeasures to an accident or a breach:</p> <p>(i) notifying the individual who may be affected ("Notice to Individual");</p> <p>(ii) reporting to the Minister of METI ("Report to METI");</p> <p>and</p> <p>(iii) making a public announcement of</p>			<p>METI Guideline lists the following example to be included in the service agreement: matters relating to reports and notifications when security accidents occur.</p> <p>Therefore, the data processor is likely to owe reporting and other obligations under the service agreement with the data controller.</p>	<p>and transmit the data;</p> <p>(iii) how to use and process the data;</p> <p>(iv) how to store and make backups of the data; and</p> <p>(v) how to delete and dispose of the data.</p>	<p>when Notice to Individual is exempted:</p> <p>(a) the lost personal data is retrieved promptly, without being seen by a third party;</p> <p>(b) the data is secured by encryption etc.; or</p> <p>(c) a third party is not able to distinguish the individual by the lost data itself (i.e., it is necessary to refer to the personal data stored by the data collector in order for the lost data to be considered as personal data).</p> <p>The METI Guideline</p>	<p>Japanese yen or less.</p> <p>In certain cases, the data controller may be liable under tort law for not implementing security safeguards to prevent loss or destruction of personal data, or for violation of privacy.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	the facts, etc. ("Public Announcement").					<p>provides no exemption from Report to METI.</p> <p>The METI Guideline provides the following criterion in order to be exempted from Public Announcement: there is no need to make a public announcement from the standpoint of preventing secondary damages.</p>		

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
<p>Lithuania</p> <p>Law on Legal Protection of Personal Data (21 January) 2003</p>	<p>The entity responsible for processing of personal data must inform State Data Protection Inspectorate in the cases when data controller breaches any of data processing requirements established by laws (including data security requirements thereto). There is no express obligation to notify individuals of a security breach. Only where the data subject requests information.</p>	N/A	<p>The notification to the State Data Protection Inspectorate must be given in written form. No other specific requirements established.</p>	N/A	<p>No specific statutory rules established. The data controllers can use their own procedures as long as they are not in conflict with law.</p>	<p>No specific statutory exemptions established.</p>	<p>Violations of the Law On Legal Protection of Personal Data shall render data controllers, data processors and other persons liable to fines. Any person who sustains damage from unlawful processing of personal data or any other acts (omissions) by the data controller, the data processor or other persons, violating the provisions of this Law are entitled to compensation for pecuniary and non-pecuniary damage caused to him.</p>	No

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Netherlands	<p>No legal requirement to notify individuals or CBP of a breach. It is advisable to notify individuals where notification helps individuals to manage their risk.</p> <p>In certain situations, if the (consequences of) the breach caused by i.e. an employee or third party may be very serious or in case of computer crime, it might be necessary to report the breach to the police.</p>	There is no prescribed time period in which the CBP/individuals should be notified but the level of risk posed by the breach must be considered and appropriate action taken depending on the seriousness of the consequences.	No legal requirements but it is advisable to inform individuals of a serious breach should including the type of information and number of records; the circumstances of the loss/release/ corruption; how and when the breach occurred; a description of the data involved; action taken to minimize/ mitigate effect on individuals involved including whether they have been informed; details of how the breach is being investigated; whether any other	There are no express reporting obligations on data processor under the Dutch Data Protection Act. Any security obligations will be derived from their contract with the data controller.	Data controllers are advised to have a security breach policy in place. It would deal with practicalities such as who should be notified within the organization in the event of an actual or suspected breach and whether press announcements may be made and by whom.	In general breaches should be disclosed, without exemptions. Though, minor breaches which do not have consequences for the individual might be exempted from disclosure. Whether disclosure is necessary depends upon the particular circumstances.	<p>Currently the CBP has no general power to impose a fine as punishment for breaches, if the data controller is able to substantiate that it took all possible (security) measures to prevent a breach.</p> <p>Individuals may bring claims for compensation for damages or distress they have suffered.</p>	No.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY

(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
			<p>regulatory body has been informed and their response; and remedial action taken to prevent future occurrence.</p> <p>When notifying individuals, clear and specific advice should be given on the steps that they can take to protect themselves and also what the Data Controller is able to do to help them, including contact details of the data controller (e.g. a helpline number).</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
<p>Poland</p> <p>Act of 29 August 1997 on Protection of Personal Data (as amended)</p>	<p>There is no statutory obligation to inform individuals nor the Polish Data Protection Authority about the breach.</p> <p>Data Controller has to undertake all necessary means to prevent further breaches.</p>	N/A	N/A	Data Processors are under obligation to comply with the provisions of data entrusting agreement executed with Data Controller. There are no reporting obligations on processors, unless the processing agreement provides otherwise.	Secondary legislation sets minimum requirements for Policies - Policies which must be complied with, nevertheless it is possible to add additional features.	N/A	<p>A Data Controller which violates, whether intentionally or unintentionally, the obligation to protect the data against unauthorized disclosure, damage or destruction, is liable to a fine, the penalty of restriction of liberty or deprivation of liberty of up to one year.</p> <p>A natural person injured by a violation of applicable regulations is entitled to bring a civil action.</p>	N/A

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Republic of Ireland Data Protection Acts 1988-2003 (the "Acts")	Notice to the individual or the regulator in respect of security breaches is not mandatory. It is recommended by the regulator (Data Protection Commissioner) that it be informed immediately. The regulator will consider with the party in breach how the persons directly affected by the security breach may best be notified. Although notice to the regulator is not mandatory, the regulator has extensive powers to prosecute for	No mandatory timing of disclosure but the regulator recommends immediate notification to it. A working group has been set up to advise on how to deal with security breaches.	By phone or email to the regulator. The regulator may ask for a detailed report including: 1) the amount and nature of the data that has been compromised; 2) what action (if any) has been taken to inform those affected; 3) a chronology of events leading up to the disclosure; and 4) a description of measures being undertaken to prevent a repetition of the incident.	There are numerous obligations on data controllers and data processors with regard to the capture, processing, transfer and retention of data, and particular additional requirements in respect of data used for electronic marketing purposes. The restrictions are extensive and onerous. Notwithstanding this, reporting of security breaches is voluntary.	There are a number of EU Model Contracts, which are in a precedent format. Any amendments to the Model Contracts require approval of the regulator although this is seldom given. There are also controller-processor agreements which must contain certain features, but for which a precedent format is not set out in legislation.	As there is no mandatory obligation, there is no exemption.	As reporting of security breaches is not mandatory, there is no liability under the Acts for failure to notify. Although data protection breaches may form part of a civil case, any damages awarded would not be under the Acts. In general, the regulator can bring criminal proceedings for breaches of the Acts, with a penalty of € 3000 on summary conviction and € 100,000 on indictment. In some circumstances, the	N/A

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	breaches of the Acts, and therefore cooperation may be advised.						management of a body corporate may be liable to be prosecuted personally as well as/instead of the body corporate, if convicted on indictment. For certain electronic marketing offences under SI 526/2008, the fines on indictment are up to £ 50,000 for an individual. For body corporates, the maximum fine is £ 250,000 (or 10% of turnover, if turnover is greater than £ 2.5 million).	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
State of Qatar (Qatar Financial Centre Data Protection Regulations and Rule Book)	None. The Qatar Financial Centre ("QFC") is a financial and business centre established in Doha by the government of the State of Qatar. The QFC operates to international standards and has its own legal infrastructure. The QFC's rules and regulations apply to all the entities licensed by it. This means that within the State of Qatar there are two legal jurisdictions operating in parallel. The QFC has Data Protection	N/A	N/A	No	N/A	N/A	A person who believes that they have been adversely affected by a breach of the Data Protection Regulations can bring a complaint before the Qatar Financial Centre Authority.	N/A

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>Regulations and a Data Protection Rulebook which apply to the entities licensed to operate in and from the QFC. The QFC's Regulations and Rulebooks are developing on an ongoing basis and so in the event of any breach of security the current rules should be checked. In relation to State of Qatar more generally, the laws relating to data protection are not contained in one law or code and in the event of any security breach Counsel should</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	take advise on the impact of such breach and the provisions of the law of the State of Qatar relating to it.							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Singapore	There is presently no overarching and comprehensive data protection legislation in Singapore, save for individual confidentiality obligations found in certain sector-specific legislation such as the Banking Act, the Statistics Act, the Official Secrets Act and the Statutory Bodies and Government Companies (Protection of Secrecy) Act. The Private Sector Model Data Protection Code ("Model Code") is a strictly voluntary	The Model Code does not provide any guidelines in this regard in the event of breach. However, as a matter of sound policy, notification should be made expeditiously, without unreasonable delay.	The Model Code does not provide any guidelines in this regard in the event of breach. However, in line with the spirit of the Model Code, notification should be made in a manner that will give the individual clear and specific details of the breach.	N/A	N/A	The Model Code does not provide any guidelines in this regard in the event of breach.	N/A	N/A

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>code. It is available for adoption by the entire private sector or may be used as a foundation on which an organization's own privacy code may be based. The Model Code does not provide guidelines on notification requirements in the event of breach.</p> <p>As a matter of sound policy, the breach should be disclosed to the individual whose personal data was subject to the breach.</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	Further, an organization must promptly, upon the individual's request, provide to that individual clear and specific information as to the disclosure of his personal data. This includes providing a list of recipients to whom the personal data are disclosed.							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Slovak Republic Act no. 428/2002 Coll. on protection of personal data	If the Data Controller employs more than five persons, it is obliged to appoint a Personal Data Protection Official to provide internal supervision and observation of the Controller's compliance. The Personal Data Protection Official is obliged to notify the Controller if he/she determines there has been a breach of the legislation. If the Controller fails to rectify the situation without undue delay, the Personal Data Protection Official is under a	According to the act no. 428/2002 Coll. on protection of personal data any disclosure/ notification related to the breach must be performed without undue delay.	Notification made by the Personal Data Protection Official related to processing of personal data delivered to the Controller or to the Data Protection Office has to be made in writing. Content of this notification is not legally prescribed.	N/A	No	If a person has a duty to notify, there is no exemption from disclosure.	Where there is a breach the Data Subject is entitled to ask the court for: a) waiver of infringement to its right to protection of personality and privacy, b) clearance of consequences of such infringement and c) appropriate compensation in accordance with Civil Code no. 40/1964 Coll.	N/A

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY

(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	duty to notify the breach to the Office for Personal Data Protection of the Slovak Republic.							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
South Africa	The legislation governing this area of law is currently before parliament and will imminently be passed. Once that legislation is in force, if it is reasonably believed that the personal information of a data subject has been accessed or acquired by an unauthorized person, the responsible party is required to notify the Regulator and the Data Subject, unless it is not possible to identify the identity of the data subject.	As soon as reasonably possible after the discovery of the compromise.	The notification to the data subject must be done in writing, in one of the following ways: mailed to the data subject's last known physical or postal address; sent by email to the data subject's last known email address; placed in a prominent position on the responsible party's website; published in the news media; or in a manner directed by the Regulator. The notification must provide sufficient information to	A data processor has the same obligations as the responsible party.	The legislation governing this area of law is currently before parliament and will imminently be passed. As such, no practices have been established as yet.	There are no provisions for absolute exemption from disclosure. A responsible party may, however, delay disclosure if directed to do so by the South African Police Services, the National Intelligence Agency or the Regulator directs that notification will impede a criminal investigation.	Upon a complaint being submitted to the Regulator, the Regulator is required to investigate the conduct of the responsible person. The Regulator will decide whether or not to take action on the complaint. Should the Regulator decide to take action, they can either refer it to a more appropriate body or investigate the matter themselves. The Regulator, in conjunction with the Courts, have wide investigatory powers, including	No

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
			enable the data subject to protect against potential consequences of the compromise, and if possible the identity of the person who had unauthorized access to the information.				the power to search and seize, and to summon witnesses. A data subject has civil remedies against the responsible parties for any breach of the security provisions, regardless of whether there is intent or negligence on the part of the responsible party. This action may be brought on behalf of the data subject by the Regulator.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Spain Organic Law 15/1993 Royal Decree 994/1999	There is generally no legal or administrative requirement to notify a security breach to the individuals or to the regulator (at least directly, see below). That said two exceptions or clarifications must be made in this regard. Firstly, and more relevantly, though data controllers suffering a security breach are not obliged to notify this to the data protection authorities, they	N/A for direct notification since there is no direct notification obligation As regards the “indirect notification” implied in the recording of a security breach in the security occurrences registry which the agency may access at any time, this recording, in accordance with section 88.7 of royal decree 1720/2007 must be immediate (the article warns it must be “updated at every time”)	N/A for direct notification since there is no direct notification obligation As regards the “indirect notification” implied in the recording of a security breach in the security occurrences registry which the agency may access at any time, this recording must be specific on the type of incident (breach) occurred, the moment it occurred, or if appropriate, was detected, the person making the	N/A for direct notification since there is no direct notification obligation The data processor is equally obliged to keep the record of the breach (or non authorized access to the data) in the security document, under the chapter “record of incidences” if this is within the processing activated that it has been retained to carry out (sections 88, 3- and 90 of royal decree 1720/2007)	N/A unless it wishes to adopt a policy requiring a greater degree of disclosure but query why it would wish to do this when the Spanish agency hasn’t established a procedure for receiving the same, and to do so would provide evidence of a breach of the legislation.	N/A for direct notification since there is no direct notification obligation. There are no exceptions to the need to recording security breaches in the security occurrences registry which the agency may access at any time	N/A for direct notification since there is no direct notification obligation. However, if a security breach occurs, it is investigated by the agency and it is shown to be the result of a breach of the regulations regarding mandatory security measures as per royal decree 1720/2007, fines may be imposed up to a sum in excess of □ 300,000	N/A for direct notification since there is no direct notification obligation. As regards the “indirect notification” implied in the recording of a security breach in the security occurrences registry which the agency may access at any time, there is no preemption. despite section 17 (3) of Directive 95/46, the practice of the Spanish data protection agency is to require Spanish controllers to comply with the

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	are obliged to record it in a security document which must at all times remain at their offices available for data protection authorities to review (the security documents are normally the first documents the staffers of the data protection agencies request at beginning an inspection). When referring to conditions in which notification” is made in the next columns we shall refer to this “indirect” notification which		notification of the security breach, to whom it was communicated, its effects and the corrective measures applied.					Spanish regulations even if all processing is made in another EU member state.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>is implied in having to record the occurrence of security breaches in the corresponding security document.</p> <p>Secondly, where the breach of data security occurs in files under the responsibility of public administrations (whether local or central) and/or governmental bodies. If the occurrence of such security breach has been revealed during an administrative procedure regarding an</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	infringement of the applicable data controllers obligations (typically, security measures) and this fact has been subject to a disciplinary procedure by the Spanish or corresponding regional data protection agency, the same is legally required to notify this to the "ombudsman" (public defender)							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY

(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Sweden The Personal Data Act 1998	No general reporting requirement.. Legislation requiring public authorities to report security breaches to data subjects has been discussed but no proposals have been put forward. Security breaches as result of crime can of course be reported to police. Prosecutable under Chapter 4 Section 9 c of the Penal Code.	N/A	N/A	No	N/A	N/A	N/A as no requirement to report. Breach of the security obligations are subject to fines and the potential for claims for damages from the individuals affected. The Agency can also prescribe security steps to be taken.	No

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
Switzerland Federal Data Protection Act 1992 ("SDPA")	There is no explicit statutory rule in the SDPA providing for notice requirements either to individuals or the regulator in case of a security breach. However, pursuant to Art. 4 Para. 2 SDPA data must be processed in good faith. In individual cases, this might imply the requirement for notification to the individuals whose data is concerned, and in some case even to a third party (e.g. a credit card	Disclosure has to be done in accordance with the principle of good faith within due course.	N/A	Data processors usually are contractually obliged to report to the data controller. Otherwise the data processor must report directly to the individuals concerned.	N/A	N/A	In case of a violation of the duty to notify, and/or the security obligation under the SDPA, damages may be claimed in a civil court. Fines for breach of the SDPA security obligations may also be levied by the regulator.	No.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>issuer in case of theft of credit card data).</p> <p>Further, a requirement for notification might arise from the principle of data security pursuant to Art. 7 SDPA, the obligation to mitigate damages pursuant to the Swiss Code of Obligations, or existing contractual obligations. Data security comprises not only technical, but also organizational measures including</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	information of relevant persons to minimize damages resulting from a security breach.							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
UK	No legal requirement to notify individuals of a breach. Whether individuals are notified depends on the nature of the breach and the level of risk posed by the breach. However, the ICO regards the notification of individuals as best practice where notification helps individuals to manage their risk. The ICO must be notified when a breach involves personal data, if a large number of people are affected, or there are very serious	There is no prescribed time period in which the ICO/individuals should be notified but the level of risk posed by the breach must be considered and appropriate action taken depending on the seriousness of the consequences.	Notification of a serious breach should include the type of information and number of records; the circumstances of the loss/release/ corruption; how and when the breach occurred; a description of the data involved; action taken to minimize/ mitigate effect on individuals involved including whether they have been informed; details of how the breach is being investigated; whether any other regulatory body has been informed and their response;	In accordance with the contract in place with the Data Controller, Data Processors must take appropriate measures against unauthorized or unlawful processing and accidental loss, destruction of or damage to personal data e.g. a policy dealing with data security breaches.	Data processors are advised to have a security breach policy in place, which should comply with the Data Protection Act 1998. It would deal with practicalities such as who should be notified within the organization in the event of an actual or suspected breach and whether press announcements may be made and by whom. In the event of an investigation by the ICO, such a policy, and evidence that it is accessible to staff, would be	There is no law at present expressly requiring notification of a breach, but the ICO must be notified of a breach if the breach has serious consequences, or involves a significant amount of personal data. As a general rule, minor breaches which do not have sufficiently serious consequences would not usually need to be disclosed but whether to disclose or not should depend upon the particular circumstances. For example, if the	Organizations can be asked by the ICO to sign an undertaking to assure the ICO that personal data will be kept securely in future. The ICO has no general power to impose a fine or other penalty as punishment for any and all breaches. However, the ICO can fine data controllers where it is satisfied that a data controller has committed a serious breach of the data protection principles; the breach was either deliberate or the data controller	No

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
	<p>consequences. In particular, if sensitive personal data is involved the consequences may be very serious. The appropriate regulatory body (if any) should be notified.</p>		<p>and remedial action taken to prevent future occurrence.</p> <p>When notifying individuals, clear and specific advice should be given on the steps that they can take to protect themselves and also what the Data Controller is able to do to help them, including contact details of the data controller (e.g. a helpline number).</p>		useful.	ICO is focusing in particular on breaches in one sector (e.g. financial services), failure to disclose what appears to be a “minor breach” may not be in the best interests of the Data Controller.	knew or ought to have known that the breach would be likely to cause significant damage or distress, but he failed to take reasonable steps to prevent the breach; and the breach was of a kind likely to cause significant damage or distress. Note that the risk of “damage or distress” is higher in the event of a breach involving sensitive personal data. In addition, the ICO has the power to issue an information notice (to find out what has happened) and	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
							an enforcement notice (to require the Data Controller to take particular steps in respect of the breach including entering into binding undertakings and to take such action as in the ICO's opinion is necessary in order to avoid further breaches). There may be other regulators, aside from the ICO, who are able to take action in the event of a breach. For example, the Financial Services Authority has issued huge fines (in excess of £1	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
							million) against banks in respect of data security breaches by them or by their data processors acting on their behalf. Further, aside from any action by the ICO or other regulators, damage to reputation is likely in the event that the breach is picked up by the press. Note that the ICO lists on its publicly available website all enforcement action which it takes against Data Controllers. It also issues press releases in the event of high	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY

(NON-US CONTENT AS OF OCTOBER 19, 2009)

Country	Notice Requirements (to who - (i)individual and (ii)regulator?)	Timing of Disclosure (does it have to be done in a particular time period?)	Form of Disclosure (does it have to be submitted in a particular way or with particular content?)	Are there reporting or other obligations on entities that maintain data (ie Data Processors)?	Existing Policies (can the controller use their own procedures as opposed to those prescribed by law?)	Exemptions from Disclosure	Damages/ Enforcement	Preemption (is there deemed compliance with the local law if you comply with another specified law?)
							profile breaches. Individuals affected by a breach are entitled to seek compensation from the Data Controller for any damage or distress they have suffered.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY: UNITED STATES

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.



INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Alaska Alaska Stat. §§ 45.48.010 to .90 (Effective July, 2009)	<p>If a breach of an information systems containing Personal Information occurs the breach must be disclosed to each Alaska resident whose personal information was subject to the breach.</p> <p>Personal information is an individuals first name or first initial and last name in combination with any of the following that is not encrypted, redacted, or secured: (1) SSN; (2) driver's or identification number; (3) financial account number or credit/debit card number with any required security code,</p>	<p>Notification must be given in the most expedient manner and without unreasonable delay.</p> <p>Notification may be delayed to participate in connection with a criminal investigation of the breach.</p>	<p>Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (only if this is the primary method of communication with the individual); 3) telephonic; or 4) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$150,000; (ii) the effected class exceeds 300,000 people; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email</p>	<p>Persons that maintain Personal Information are not required to comply with the notice requirements. Instead, upon discovery of the breach they must notify the information owner about the breach and cooperate to the extent necessary to allow the information owner to satisfy the notice requirements.</p>		<p>Disclosure is not required if, after an appropriate investigation, and after written notification to the attorney general, it is determined that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach.</p>	<p>Violation of the statute is considered a violation of Alaska's unfair or deceptive practices act. However, the information owner is not subject to civil penalties and damages under the statute and instead is liable to the state for a civil penalty of up to \$500 for each Alaska resident who was not notified in an amount not to exceed \$50,000. Damages that</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>access code, or password; (4) passwords, PINS, or other access codes for financial accounts.</p> <p>f a security breach requires notice to more than 1,000 individuals notice of the breach must also be provided to all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices. Names and personal information of individuals subject to the breach are not required.</p> <p>Notice to Other Entities Includes information “in any form”.</p>		<p>notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>			<p>No likelihood of harm PLUS written notification to AG.</p>	<p>can be awarded under the statute are limited to actual to actual economic damages that do not exceed \$500.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Arizona Ariz. Rev. Stat. § 44-7501	Notification must be given to affected persons by those who own or license unencrypted data that includes Personal Information once that person becomes aware of an incident of unauthorized acquisition AND access to unencrypted information that includes Personal Information. Personal Information is any individual's first name or first initial and last name in combination with any of the following element that is not encrypted, redacted or secured: (1) SSN; (2) driver's license number or identification number; (3) financial account number or credit/debit card number with any	Notification must be given in the most expedient manner and without unreasonable delay. Notification may be delayed to participate in connection with a criminal investigation of the breach.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (only if this is the primary method of communication with the individual); 3) telephonic; or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$100,000; (ii) the effected class exceeds 100,000 people; or (iii) insufficient contact information. Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major	Persons that maintain unencrypted Personal Information are obligated to cooperate with the owner of the information with respect to any breach. The person maintaining the information is only required to provide notice of a breach if the agreement with the owner of the information so requires.	If notification procedures are included in a person's security policy, that person is in compliance with the notification requirements in Arizona if individuals are notified in accordance with those procedures.	Disclosure is not required if, after a reasonable investigation, it is determined that a breach did not occur or is not reasonably likely to occur.	Actual damages and a civil penalty not to exceed \$10,000 per breach or series of breaches of a similar nature that are discovered in a single investigation.	If a person is in compliance with guidelines established by the primary or functional federal regulator, such person is deemed in compliance with this law.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	required security code, access code or password.		statewide media.					
Arkansas Ark. Code §§ 4-88-113, -10-105	<p>Breaches of security systems that include Personal Information must be disclosed to the affected parties following discovery of the breach if unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following non-redacted or non-encrypted elements: (1) SSN; (2) driver's license number or Arkansas identification card number; (3) account number or credit/debit</p>	<p>Notification must be given in the most expedient manner and without unreasonable delay.</p> <p>Notification may be delayed to participate in connection with a criminal investigation of the breach.</p>	<p>Disclosure to be given in one of the following forms:</p> <p>1) written notice; 2) electronic notice (if consistent with federal electronic signature laws); or 3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 people; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is</p>	Any person that maintains Personal Information must give notice to the person that owns the information immediately following discovery of a breach.	Data owners are permitted to utilize their own notification procedures if the procedures are part of an information security policy and the policy is otherwise consistent with the timing required by Arkansas law.	No notice is required if, after a reasonable investigation, the person determines there is no reasonable likelihood of harm	Violators of law are guilty of a Class A misdemeanor. Civil enforcement actions may also be brought.	Arkansas law does not apply to businesses regulated by a state or federal law that provides greater protection to Personal Information and at least as thorough disclosure requirements than provided by Arkansas Law.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	card number with any required security code, access code or password; or (4) medical information. PI definition includes health data.		maintained); and (c) notification to major statewide media.					
California Cal. Civ. Code § 1798.82	Law applies to any Company that conducts business in California. If an owner (i) conducts business in CA; (ii) owns or licenses unencrypted computer information; and (iii) the data contains Personal Information regarding a resident, then disclosure is required. Also, if there is a security breach of a system containing Personal Information and it is known or reasonably believed that Personal Information	Disclosure to be made as expediently as possible, and without unreasonable delay, unless there is a concern that disclosure will impede a criminal investigation.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if consistent with federal electronic signature laws); or 3) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 people; or (iii) insufficient contact information. Substitute notice must	Any person that maintains Personal Information must give notice to the person that owns the information immediately following discovery of a breach.	Data owners may continue using their own disclosure regimes if they are part of a broader information security policy, but only if the policy is consistent with the timing requirements of California law.	Compliance cannot be waived by the affected individual.	Any consumer injured by a violation of this law can bring a civil action to recover damages.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>has been acquired, then disclosure must also be made.</p> <p>Personal Information means an individual's first name or middle initial combined with a last name and any of the following: (1) SSN; (2) CA driver's license number or identification card number; (3) account number or credit/debit card number with any required security code, access code or password; (4) medical information; (5) health insurance information.</p> <p>PI definition includes health and health insurance information.</p>		<p>consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>					
Cal. Health & Safety Code § 1280.15	A clinic, health facility, home health agency, or hospice licensed under California law must	Report to State Department of Public Health must be made no later					The State Department of Public Health, after	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>prevent unlawful or unauthorized access to, use of, and disclosure of patients' medical information. Such organizations must also report to State Department of Public Health and to the affected patient or patient's representative any unlawful or unauthorized access, use, or disclosure of medical information.</p> <p>Medical information means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment.</p>	<p>than 5 days after the unlawful or unauthorized access, use, or disclosure was detected.</p> <p>Report must be made to affected patient or patient's representative at last known address no later than 5 days after the unlawful or unauthorized access, use, or disclosure was detected.</p>					<p>investigation, may assess an administrative penalty for a violation of up to \$25,000 per patient whose medical information was unlawfully or without authorization accessed, used, or disclosed; and up to \$17,500 per subsequent occurrence of unlawful or unauthorized access, use, or disclosure of that patient's medical information.</p> <p>Following the initial 5 day reporting period, the State Department of Public Health</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	Individually identifiable means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity.						<p>may assess a penalty in the amount of \$100 for each day that the unlawful or unauthorized access, use, or disclosure is not reported.</p> <p>The total combined penalty assessed by the State Department of Public Health must not exceed \$250,000 per reported event.</p> <p>Within 10 days of receipt of a penalty assessment a hearing may be requested to dispute a determination by the State Department of Public Health</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
							<p>regarding a failure to prevent or failure to timely report unlawful or unauthorized access to, use of, or disclosure of patients' medical information, or the imposition of a penalty.</p> <p>In lieu of disputing the determination of the State Department of Public Health regarding a failure to prevent or failure to timely report unlawful or unauthorized access to, use of, or disclosure of patients' medical information, transmit to the</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
							<p>department 75% of the total amount of the administrative penalty for each violation, within 30 days of receipt of the administrative penalty.</p> <p>The State Department of Public Health may refer violations to the office of Health Information Integrity for enforcement.</p>	
Colorado	<p>Notice requirements apply to entities that conduct business in Colorado who own or license computerized data that includes Personal Information.</p> <p>If notification is to be given to more than</p>	<p>Disclosure to be made as expeditiously as possible, and without unreasonable delay, unless there is a concern that disclosure will impede a criminal</p>	<p>Disclosure to be given in one of the following forms:</p> <p>1) written notice; 2) telephonic notice; 3) electronic notice (if it is a primary means of communication or it is consistent with federal electronic signature</p>	<p>Any person that maintains Personal Information must give notice to the person that owns the information immediately following discovery of a breach, if misuse of Personal</p>	<p>Data owners who maintain their own notification procedures which are consistent with the timing requirements of Colorado law are deemed to be in compliance with</p>	<p>No notification is required if it is determined (after reasonable investigation) that the breach did not occur or is not reasonably likely to occur.</p>	<p>The Attorney General may bring an action to address violations of this section and for other relief that may be appropriate to ensure compliance with</p>	<p>Data owner who is regulated by state or federal law and who maintains procedures for breaches pursuant to the laws, rules, regulations, guidance or guidelines</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>1,000 Colorado residents, the data owner must also notify all consumer reporting agencies.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following non-redacted or non-encrypted elements: (1) SSN; (2) driver's license number or identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p> <p>Notice to Other Entities is Required.</p>	investigation.	<p>laws); or 4) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 250,000 Colorado residents; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	Information is likely to occur.	the notice requirements if notification is provided in accordance with its policies.		the law.	established by the applicable principal regulator is deemed to be in compliance with this statute.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Connecticut Conn. Gen. Stat. Ann. § 36a-701b	<p>Notice requirements apply to entities that conduct business in Connecticut who own, license or maintain computerized data that includes Personal Information.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following: (1) SSN; (2) driver's license number or identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p>	Disclosure to be made without unreasonable delay, subject to delay at the request of law enforcement agencies and the completion of investigations to determine nature of breach. If notice is delayed, may only be given after approval by the applicable law enforcement agency.	<p>Disclosure to be given in one of the following forms: 1) written notice; 2) telephonic notice; 3) electronic notice (if it is consistent with federal electronic signature laws); or 4) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	Any person that maintains Personal Information must give notice to the person that owns the information immediately following discovery of a breach, if the Personal Information was, or is reasonably believed to have been accessed by an unauthorized person.	<p>Data owners who maintain their own notification procedures which are consistent with the timing requirements of Connecticut law are deemed to be in compliance with the notice requirements if notification is provided in accordance with its policies.</p> <p>Any business that complies with procedures pursuant to GLB are deemed to be in compliance with Connecticut law.</p>	Notice is not required if after investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person determines that it will not result in harm to the affected individuals.	Failure to comply with Connecticut law is considered an unfair trade practice for purposes of section 42-110b of Connecticut's general statutes and will be enforced by the Attorney General.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Delaware Del. Cod. Ann. tit. 6, §§ 12B-101 to -104	<p>Notice requirements apply to entities that conduct business in Delaware who own, license or maintain computerized data that includes Personal Information.</p> <p>A breach of a security system means the unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of the Personal Information maintained by an individual.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following, when either the name or the element is not</p>	<p>Disclosure to be made in the most expedient time and without unreasonable delay, consistent with legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and restore the integrity of the system. If notice is delayed by law enforcement, may only be given after approval by the applicable law enforcement agency.</p>	<p>Disclosure to be given in one of the following forms: 1) written notice; 2) telephonic notice; 3) electronic notice (if it is consistent with federal electronic signature laws); or 4) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$75,000; (ii) the effected class exceeds 100,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c)</p>	<p>Any person that maintains Personal Information must give notice to the person that owns the information immediately following discovery of a breach, if the Personal Information was, or is reasonably believed to have been acquired by an unauthorized person.</p>	<p>Data owners who maintain their own notification procedures which are consistent with the timing requirements of Delaware law are deemed to be in compliance with the notice requirements if notification is provided in accordance with its policies.</p>		<p>Enforcement actions may be brought by Delaware residents, in which case damages are tripled and reasonable attorneys' fees are also recoverable.</p> <p>Attorney General may also bring actions to address violations.</p>	<p>A data owner who is complying with provisions of a federal or state law that provide greater protection than Delaware law will be deemed to be in compliance with Delaware law. However, this does not relieve an individual or a commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of Personal Information.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>encrypted: (1) SSN; (2) DE driver's license number or DE identification card number; (3) account number or credit/debit card number with any required security code, access code or password; or (4) individually identifiable information regarding medical history.</p> <p>PI definition includes health data.</p>		notification to major statewide media.					
Florida Fla. Stat. § 817.5681	<p>Notice is required if an unauthorized person obtains Personal Information from a system that contains unencrypted computerized data.</p> <p>A reasonable belief of breach is sufficient to trigger notice</p>	Notification is to be made within 45 days of the discovery of the breach, subject to: (i) legitimate needs of law enforcement, and (ii) measures needed to determine nature, presence and scope	<p>Disclosure to be given in one of the following forms:</p> <p>1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws); or 3) substitute notice.</p> <p>Substitute notice is</p>	Any person that maintains Personal Information for others must give notice to the person that owns the information within 10 days of receiving actual knowledge or a reasonable belief of a breach. Either	Data owners who maintain their own notification procedures which are consistent with the timing requirements of Florida law are deemed to be in compliance with the notice	No notice is required if, after consultation with law enforcement, it is reasonably determined that the breach has not and will not likely result in harm to the affected	The notice must be given within 45 days of the discovery of the breach unless one of these two exceptions applies. If notice is not given within this timeframe there are civil	A data owner who is regulated by federal law and who maintains procedures for breaches pursuant to the laws, rules, regulations, guidance or guidelines established by the

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>requirements.</p> <p>If the breach affects more than 1,000 Florida residents, notification must also be given to the appropriate credit reporting agencies.</p> <p>Personal Information means an individual's first name or middle initial combined with a last name and any of the following: (1) SSN; (2) FL driver's license number or identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p> <p>Notice to other entities required.</p>	<p>of the breach and to restore the reasonable integrity of the system.</p> <p>The following civil penalties apply to untimely notice: (1) \$1,000 per day for the first 30 day period; (2) \$50,000 for each 30 day period thereafter up to 180 days; or (3) up to \$500,000 if notice is not given within 180 days.</p> <p>Penalties are per breach, not per individual.</p> <p>Notice within 45 days, with exceptions.</p>	<p>permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>the owner of the information or the party maintaining the information may provide notice, though if there is no agreement regarding obligated party the entity with the direct business relationship with the consumer must provide the notice.</p>	<p>requirements if notification is provided in accordance with its policies.</p>	<p>individuals.</p> <p>If this exemption is relied upon, it must be put in writing and maintained by the Company for a period of 5 years.</p>	<p>penalties that are available, up to a total of \$500,000, as follows: (i) \$1,000 per day for the first 30 period; (ii) \$50,000 for each 30 period thereafter up to 180 days; or (iii) up to \$500,000 if notice is not given within 180 days.</p> <p>The penalties apply per breach, not per effected individual. These penalties do not apply to the government, but can apply to certain entities that have entered a contract with the government.</p>	<p>applicable principal regulator is deemed to be in compliance with this statute.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Georgia Ga. Code Ann. §§ 10-1-912, 46-5-210	<p>A person that maintains computerized data that includes Personal Information of individuals must give notice of any breach of the security of the system following discovery or notification of the breach to any resident of Georgia whose Personal Information was or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>If notification must be given to more than 10,000 Georgia residents with respect to any single breach, notice must also be given to all consumer reporting agencies.</p> <p>A breach is an unauthorized</p>	<p>Disclosure to be made in the most expedient time and without unreasonable delay, consistent with legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and restore the integrity of the system. If notice is delayed by law enforcement, may only be given after approval by the applicable law enforcement agency.</p>	<p>Disclosure to be given in one of the following forms: 1) written notice; 2) telephonic notice; 3) electronic notice (if it is consistent with federal electronic signature laws); or 4) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$50,000; (ii) the effected class exceeds 100,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>Any person that maintains Personal Information must give notice to the person that owns the information within 24 hours following discovery of a breach, if the Personal Information was, or is reasonably believed to have been acquired by an unauthorized person.</p>	<p>Data owners who maintain their own notification procedures which are consistent with the timing requirements of Georgia law are deemed to be in compliance with the notice requirements if notification is provided in accordance with its policies.</p>		<p>Violations constitute an unfair or deceptive practice in consumer transactions under the Fair Business Practices Act.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>acquisition of computerized data that compromises the security, confidentiality or integrity of Personal Information.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following, when either the name or the element is not encrypted: (1) SSN; (2) GA driver's license number or GA identification card number; (3) account number or credit/debit card number if they can be used without access codes or passwords; (4) account passwords or personal identification numbers or other access codes; or (5) any of the above when not in connection with the first</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	name or last name, if the information would be sufficient to perform or attempt to perform identity theft against the person. Notice to Other Entities is Required.							
Hawaii Haw. Rev. Stat. §§ 487N-1 to -4	Notice requirements apply to any business that owns or licenses Personal Information of residents of Hawaii, any business that conducts business in Hawaii that owns, licenses or maintains computerized data that includes Personal Information and governmental agencies that collect Personal Information. If notification must be given to more than 1,000 Hawaii residents with respect to any single breach, notice	Disclosure to be made without unreasonable delay, subject to delay at the request of law enforcement agencies and the completion of investigations to determine nature of breach. If notice is delayed, may only be given after approval by the applicable law enforcement agency.	Disclosure to be given in one of the following forms: 1) written notice; 2) telephonic notice; 3) electronic notice (if it is consistent with federal electronic signature laws); or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$100,000; (ii) the effected class exceeds 200,000 persons; or	Any person that maintains Personal Information must give notice to the person that owns the information immediately following discovery of a breach.			The Attorney General or the Director of the Office of Consumer Protection may bring actions under this law. Damages are limited to actual damages sustained as a result of violation.	The following are deemed in compliance: 1) a financial institution that is subject to the Federal Guidance on Response Programs for Unauthorized Access to Consumer Information and Customer Notice published by the Federal Register on March 29, 2005; and 2) health plans and healthcare providers that are subject to

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>must also be given to the State of Hawaii's Office of Consumer Protections and all consumer reporting agencies.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following, when either the name or the element is not encrypted: (1) SSN; (2) HI driver's license number or HI identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p> <p>Notice to Other Entities is Required.</p>		<p>(iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p> <p>Notice must be clear and include the following: (i) the incident in general terms; (ii) the type of Personal Information that was subject to the breach; (iii) the acts of the business to protect the Personal Information; (iv) a telephone number to call for further information; and (v) advice that directs the person to remain vigilant by reviewing</p>					and in compliance with the standards for privacy of individually identifiable health information and the security standards for the protection of electronic health information.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	Applies to all forms of data.		account statements and monitoring free credit reports. Specific Notice requirements.					
Idaho Idaho Code Ann. §§ 28-51-105 to -107	Any agency, individual or commercial entity that conducts business in Idaho that owns or licenses computerized data that includes Personal Information about an Idaho resident must give notice to the affected resident if it becomes aware of a breach of the security of the system and determines the misuse has occurred or is reasonably likely to occur. Personal Information means an individual's first name or first initial	Disclosure to be made in the most expedient time and without unreasonable delay, consistent with legitimate needs of law enforcement. If notice is delayed by law enforcement, notice may only be given after approval by the applicable law enforcement agency.	Disclosure to be given in one of the following forms: 1) written notice; 2) telephonic notice; 3) electronic notice (if it is consistent with federal electronic signature laws); or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$25,000; (ii) the effected class exceeds 50,000 persons; or (iii) insufficient contact information. Substitute notice must consist of: (a) email	Persons that maintain computerized data owned by others that includes Personal Information must give notice to and cooperate with the owner or licensee of the information of any breach following discovery of the breach if misuse of Personal Information is reasonably likely to occur	Data owners who maintain their own notification procedures which are consistent with the timing requirements of Idaho law are deemed to be in compliance with the notice requirements if notification is provided in accordance with its policies.		Enforcement actions are brought by the primary regulator; fines may not exceed more than \$25,000 per breach.	A data owner who is regulated by state or federal law and who maintains procedures for breaches pursuant to the laws, rules, regulations, guidance or guidelines established by the applicable principal regulator is deemed to be in compliance with this statute if the entity complies with the maintained procedures.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	and last name in combination with any of the following, when either the name or the element is not encrypted: (1) SSN; (2) driver's license number or ID identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.		notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.					
Illinois 815 Ill. Comp. Stat. 530/5 to /25	Anyone that handles, collects, disseminates or otherwise deals with nonpublic Personal Information that it either owns or licenses is obligated to notify residents of any breach of the security of system data. A breach means the unauthorized acquisition of computerized data that compromises the	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws); or 3) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the	Persons that maintain computerized data owned by others that includes Personal Information must give notice to and cooperate with the owner or licensee of the information of any breach following discovery of the breach if the Personal	Data owners who maintain their own notification procedures which are consistent with the timing requirements of Illinois law are deemed to be in compliance with the notice requirements if notification is provided in accordance with its		Violations are considered unlawful practices under the Consumer Fraud and Deceptive Business Practices Act.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>security, confidentiality or integrity of Personal Information.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following, when either the name or the element is not encrypted: (1) SSN; (2) driver's license number or state identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p>	of the system.	<p>effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	Information was, or is reasonably believed to have been, acquired by an unauthorized person.	policies.			
Indiana Ind. Code §§ 24-4.9-1 to -5	Any business that owns or licenses computerized data that includes Personal Information must disclose a breach of the security of the system if	<p>Notification of breach must be provided without unreasonable delay.</p> <p>A delay is reasonable if the</p>	<p>Disclosure to be given in one of the following forms:</p> <p>1) mail; 2) telephone; 3) facsimile; or 4) electronic mail, if the</p>	A person that maintains computerized data must notify the owner or licensee if the person discovers that personal	Data owners are not required to make separate disclosures if they maintain their own disclosure procedures that are		The attorney general may bring an action to obtain any or all of the following: (1) an injunction to enjoin future	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>unencrypted information was or may have been acquired by unauthorized persons or if encrypted information was or may have been acquired by unauthorized persons with access to the encryption key when the business knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud.</p> <p>If the notification is to be given to more than 1,000 individuals, the business must disclose to each consumer reporting agency information necessary to assist in preventing fraud, including personal information of</p>	<p>delay is (1) necessary to restore the integrity of the computer system; (2) necessary to discover the scope of the breach; or (3) in response to a request from the attorney general or law enforcement to delay disclosure because disclosure will (A) impede a criminal or civil investigation or (B) jeopardize national security.</p> <p>A business must make a disclosure or notification as soon as possible after (1) delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach; or (2)</p>	<p>business has the electronic mail address of the affected individual.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; or (ii) the effected class exceeds 500,000 persons..</p> <p>Substitute notice must consist of: (a) conspicuous posting on website (if one is maintained); and (b) notification to major statewide media.</p>	<p>information was or may have been acquired by an unauthorized person.</p>	<p>at least as stringent as the disclosure requirements in (1) this statute; (2) the federal USA Patriot Act; (3) Executive Order 132254; (4) the federal Driver's Privacy Protection Act; (5) FACTA; (6) the federal Financial Modernization Act; or (7) HIPAA; and the procedure is complied with and requires that Indiana residents be notified.</p> <p>Financial institutions are not required to make disclosures under this law if they comply with the disclosure requirements prescribed under</p>		<p>violations; (2) a civil penalty not to exceed \$150,000 for each failure to make a required disclosure or notification in connection with a related series of breaches; and (3) the attorney general's reasonable costs in (A) the investigation each failure to make a required disclosure or notification in connection with a related series of breaches; and (B) maintaining the action.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>the individuals affected by the breach.</p> <p>A breach is an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of Personal Information, including the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in computerized format.</p> <p>Personal Information means an individual's SSN that is not encrypted or redacted or an individual's first name or first initial and last name in</p>	<p>the attorney general or a law enforcement agency gives notice that delay will no longer impede a criminal or civil investigation or jeopardize national security.</p>			<p>the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice or the Guidance Response Programs for Unauthorized Access to Member Information and Member Notice.</p>			

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>combination with any of the following: (1) driver's license number or state identification card number; (2) state identification card number; (3) credit card number; or (4) financial account number debit card number with any required security code, password, or access code.</p> <p>Notice to Other Entities is Required.</p> <p>Covers non-electronic information if it was originally computerized data.</p>							
Iowa Iowa Code §§ 715C.1 to .2	Any person that owns or licenses computerized data that includes Personal Information that is used in the course of that person's business, vocation, occupation, or volunteer	Notification must be made in the most expeditious manner possible and without unreasonable delay consistent with the legitimate needs of	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws); or	Any person that maintains Personal Information must notify the owner or licensor of the breach immediately following discovery of the breach of		Notification is not required if, after an appropriate investigation or after consultation with federal, state, or local agencies	Attorney general may enforce violations of the statute and may obtain an order that a party violating the statute pay	A person who complies with security breach notification requirements that provide greater personal protection to personal

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>activities must give notice of a breach of the security system to any individual whose Personal Information was breached.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following: (1) SSN; (2) driver's license or identification number; (3) financial account, credit/debit card number in combination with the required security code, access code, or password for that account; (4) unique electronic identifier or routing code; (5) unique biometric data, such as, fingerprints or retina images.</p>	<p>law enforcement, any measures necessary to sufficiently determine contact information, and to restore the reasonable integrity, security, and confidentiality of the data.</p> <p>Notice requirements may be delayed if a law enforcement agency determines that notification will impede a criminal investigation and the agency makes a written request that notification be delayed.</p>	<p>3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 350,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p> <p>Notice must include (1) a description of the breach of security; (2) approximate date of the breach; (3) type of personal information obtained as a result of the breach; (4) contact</p>	<p>security contained Personal Information.</p>		<p>responsible for law enforcement it is determined that no likelihood of financial harm to the consumer whose Personal Information was breached will result from the breach.</p>	<p>damages to the attorney general on behalf of a party injured by the violation.</p>	<p>information and at least as thorough disclosure requirements than that provided by this law under rules, regulations, procedures, guidance, or guidelines established by that person's primary federal regulator or state or law need not comply with the statute.</p> <p>A person who is subject to complies with regulations promulgated pursuant to GLB is also exempted from this law.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	PI definition includes biometric data or unique electronic identifier.		information for consumer reporting agencies; (5) advice to the consumer to report suspected identity theft to local law enforcement or the attorney general. Notice content requirements.					
Kansas Kan. Stat. Ann. § 50-7a02	Any person that conducts business in Kansas that owns or licenses computerized data that includes Personal Information must disclose a breach of the security of the system after determining that the misuse of information has occurred or is reasonably likely to occur. If the notification is to be given to more than 1,000 individuals, it must also be given to all	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed by law enforcement	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws); or 3) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$100,000; (ii) the effected class exceeds 5,000 persons; or (iii) insufficient contact information.	Any person that maintains Personal Information must give notice to the person that owns the information immediately following discovery of a breach, if the Personal Information was, or is reasonably believed to have been acquired by an unauthorized person.	Data owners who maintain their own notification procedures which are consistent with the timing requirements of Kansas law are deemed to be in compliance with the notice requirements if notification is provided in accordance with its policies.		Attorney General may bring claims under this statute.	A data owner who is regulated by state or federal law and who maintains procedures for breaches pursuant to the laws, rules, regulations, guidance or guidelines established by the applicable principal regulator is deemed to be in compliance with this statute if the entity complies with the maintained procedures.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>consumer reporting agencies.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or state identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p> <p>Notice to Other Entities is Required.</p>	agencies.	Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.					
Louisiana La. Rev. Stat. Ann. §§ 51:3071 to :3077	Any person that conducts business in Louisiana that owns or licenses computerized data that includes Personal Information	Notification of breach must be provided without unreasonable delay, consistent with the legitimate needs of	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is consistent with	Persons that maintain computer data that it does not own or license that includes Personal Information must	If a person maintains a notification procedures as part of its information security policy for	No disclosure required if, after reasonable investigation, it is determined that there is no	Affected individuals may recover actual damages.	A financial institution that is subject to the Federal Guidance on Response Programs for Unauthorized

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>must disclose a breach of the security of the system if it is known or is reasonably believed that the data was acquired by an unauthorized person.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number; or (3) account number or credit/debit card number with any required security code, access code or password.</p>	<p>law enforcement and any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data. Notification may be delayed by law enforcement.</p>	<p>federal electronic signature laws); or 3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>notify the owner or licensee of the Personal Information if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of a security system.</p>	<p>Personal Information, it may be utilized if it is otherwise consistent with the timing requirements of this law.</p>	<p>reasonable likelihood of harm to the customer.</p>		<p>Access to Consumer Information and Customer Notice published by the Federal Register on March 29, 2005 is deemed to be in compliance with this statute.</p>
<p>Maine</p> <p>Me. Rev. Stat. Ann. tit. 10, §§ 1346 to 1349</p>	<p>Any person that conducts business in Maine that owns or licenses computerized data that includes Personal Information</p>	<p>Notification of breach must be provided in the most expedient time possible and without</p>	<p>Disclosure to be given in one of the following forms: 1) written notice; or 2) substitute notice.</p>	<p>Persons that maintain computer data that it does not own or license that includes Personal Information must</p>			<p>Law is maintained by the Office of Consumer Credit Regulation; fines are up to \$500</p>	<p>A person that complies with security breach notification requirements of rules, regulations,</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>must disclose a security breach involving Personal Information if it is known or is reasonably believed that the data was acquired by an unauthorized person.</p> <p>A security breach is the compromise of the security, confidentiality or integrity of Personal Information that results in unauthorized acquisition of access to Personal Information or that creates a reasonable basis that such acquisition has occurred.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2)</p>	<p>unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed by law enforcement agencies.</p> <p>Delay of notification pursuant to law enforcement request is limited to a maximum of 7 business days. (Maine LD 970, enacted May 19, 2009).</p>	<p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>notify the owner or licensee of the Personal Information if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person through a breach of a security system.</p>			<p>per violation, up to a maximum of \$2,500 per day. Civil actions are also permitted.</p>	<p>procedures, or guidelines established under federal or Maine law is deemed to be in compliance with this statute as long as the notification procedures are at least as protective as the notification requirements of this statute.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	driver's license number or state identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.							
Maryland Md. Code. Ann., Com. Law §§ 14-3504 to -3508	Any business that owns or licenses computerized data that includes Personal Information of Maryland residents must disclose a breach of a security system if it is determined that there has been or is reasonably likely to occur a misuse of the individual's Personal Information. Compliance cannot be waived. A breach of a security system is an	Prior to providing notice the business must provide notice of the security breach to the Office of the Attorney General. Notification must be given as soon as practicable after conclusion of the investigation. Notice can be delayed if instructed by law enforcement agencies.	Disclosure to be given in one of the following forms: 1) written notice; 2) telephonic notice; 3) electronic notice (if it is consistent with federal electronic signature laws and the individual has so consented or business is conducted primarily through internet account transactions); or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing	Persons that maintain computerized data owned by others that includes Personal Information must give notice to and cooperate with the owner or licensee of the information of any breach following discovery of the breach if misuse of Personal Information is reasonably likely to occur	If it is reasonably determined that no misuse has occurred or is reasonably likely to occur, no notification is required. If it is determined that no notification needs to be given, a written record to that affect must be maintained by the Company.		Violation is an unfair or deceptive trade practice in Maryland.	A data owner who is regulated by state or federal law and who maintains procedures for breaches pursuant to the laws, rules, regulations, guidance or guidelines established by the applicable principal regulator is deemed to be in compliance with this statute if the entity complies with the maintained procedures.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of Personal Information.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or state identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p> <p>If a business is required to give notice of a breach to 1,000 or more individuals the</p>		<p>notice would exceed \$100,000; (ii) the effected class exceeds 175,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p> <p>Disclosure must include:</p> <p>1) a description of the information that was, or reasonably believed to have been, acquired; 2) contact information for the person making the disclosure; 3) the toll-free numbers and addresses for the major reporting</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	business must also notify without unreasonable delay each consumer reporting agency that complies and maintains files on consumers on a nationwide basis of the timing, distribution, and content of the notices. Notice to Other Entities is Required.	Notice to State AG required before notice goes to individuals.	agencies; 4) toll-free numbers, addresses and website addresses for the FTC and the Office of the Attorney General; and 5) a statement that an individual can obtain information from these sources to avoid identity theft. Notice content required.					
Massachusetts Mass. Gen. Laws ch. 93H §§ 1 to 6	A person who owns or licenses Personal Information of Massachusetts residents must provide notice as soon as practicable once it is known or there is reason to know of a breach of security or that Personal Information of the resident was acquired or used by an unauthorized person or for an unauthorized	Must be given as soon as practicable. Notice may be delayed at the request of law enforcement agencies. Notice must include: (1) the consumer's right to obtain a police report; (2) how a consumer requests a security freeze; and	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws); or 3) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds	Persons that maintain computerized data owned or licensed by others that includes Personal Information must give notice as soon as practicable once it is known or there is reason to know of a breach of security or that Personal Information of the resident was acquired or used by	The law does not relieve any person from the duty to comply with any requirements of the law.		The Attorney General may bring suits for violation.	A person who maintains procedures for responding to a breach of security pursuant to federal laws, rules and regulations is deemed to be in compliance if the person notifies the affected Massachusetts residents in accordance with maintained or

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>person.</p> <p>Notice must also be given to Attorney General and the director of consumer affairs and business regulation. The notice must include the nature of the breach of security or unauthorized acquisition or use, the number of residents affected and any steps the person or agency has taken or plans to take relating to the incident. Upon receipt, the director of consumer affairs and business regulation must identify any relevant consumer reporting agency or state agency, as deemed appropriate by the director, and forward the names of the identified consumer reporting agencies and</p>	<p>(3) fees required to be paid to any of the consumer reporting agencies.</p>	<p>500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p> <p>Notification cannot include the nature of the breach or unauthorized acquisition or use or the number of residents of Massachusetts affected by the breach.</p>	<p>an unauthorized person or for an unauthorized person.</p>				<p>required procedures. Must also notify the attorney general and the director of the office of consumer affairs and business regulation of the breach as soon as practicable.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>state agencies to the notifying person or agency.</p> <p>A breach of a security system is an unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality or integrity of Personal Information.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or state identification card number; or (3) account number or credit/debit card</p>		<p>Notice content required.</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>number with any required security code, access code or password.</p> <p>Notice to Other Entities is Required.</p> <p>Includes non-electronic data.</p>							
Michigan Mich. Comp. Laws §§ 445.63, .72	Any person that discovers a security breach in a database it owns or licenses, or that receives notice of a security breach, must provide written notice of the breach to Michigan residents whose Personal Information was accessed by an unauthorized person or that the Personal Information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key,	Notice must be given without unreasonable delay after an investigation has been completed to determine the scope of the security breach and restore reasonable integrity of the system. Notice may also be delayed at the request of law enforcement.	Disclosure to be given in one of the following forms: 1) written notice; 2) telephonic notice (if not prohibited by federal or state law; message may not be given by a recorded message; individual must have consented to notification via telephone, or if consent was not previously given the notification is also followed up with a written notification if the notice does not result in a live	Persons that maintain computerized data owned by others that includes Personal Information must give notice to and cooperate with the owner or licensee of the information of any breach following discovery of the breach unless it is determined that the security breach has not or is not likely to cause substantial loss or injury to, or	Notice may be provided pursuant to an agreement with a third-party if the notice does not conflict with any requirement of the law.	Financial institutions that are subject to, and have notification procedures in place that are subject to examination by the financial institution's appropriate regulator for compliance with, the interagency guidance on response programs for unauthorized	A civil fine of \$250 may be ordered for each failure to provide notice, with the aggregate liability for multiple violations out of the same breach not to exceed \$750K.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>unless it is determined that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or state identification card number; (3) demand deposit or other financial account number or credit/debit card number with any required security code, access code or password.</p>		<p>conversation within 3 days of the initial attempt);</p> <p>3) electronic notice (if the individual has so consented, an existing business relationship exists that includes periodic email communications which causes the person to believe the email address is correct or the person's business is conducted primarily through internet account transactions); or</p> <p>4) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p>	<p>result in identity theft.</p>		<p>access to customer information and customer notice prescribed by the board of governors of the federal reserve system and the other federal bank and regulatory agencies.</p> <p>Agencies in compliance with HIPAA are also considered to be in compliance.</p>		

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>If notice is required to more than 1,000 Michigan residents or if the person or entity is not subject to the GLB must notify each consumer reporting agency that compiles and maintains consumer files on a nationwide basis. The notice must include the number of notices sent and the timing of the notices.</p> <p>Notice to Other Entities is Required.</p>		<p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media, but the notice must include a telephone number or website to obtain additional information.</p> <p>Notice must be written in a clear and conspicuous manner and:</p> <ol style="list-style-type: none"> 1) describe the security breach in general terms; 2) describe the type of Personal Information that is the subject of the unauthorized access or use; 3) generally describe what the agency or person providing the notice has done to 					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
			<p>protect the information from future breaches; 4) include a telephone number where a recipient may obtain assistance or additional information; and 5) remind recipients the need to remain vigilant for incidents of fraud and identity theft.</p> <p>The above must be communicated if notice is provided via the telephone.</p> <p>Notice content required.</p>					
Minnesota Minn. Stat. § 325E.61	Any business that owns or licenses computerized data that includes Personal Information of Minnesota residents must disclose a breach of a security system to such person if it is determined that such	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws and is the primary method of communication with	Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of	If a person maintains a notification procedures as part of its information security policy for Personal Information, it may be utilized if it is otherwise		Violations are enforced by the Attorney General.	Any financial institution covered by GLB. Covered entities under HIPAA.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>person's Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>If notification is to more than 500 persons at one time, the person giving notice shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.</p> <p>A breach of a security system is an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of Personal Information.</p>	<p>scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed by law enforcement agencies.</p>	<p>the person); or 3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>any breach following discovery of the breach if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>consistent with the timing requirements of this law.</p>			

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key was also acquired: (1) SSN; (2) driver's license number or MN identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p> <p>Notice to Other Entities is Required.</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Missouri H.B. 62, 95th Gen. Assem., Reg. Sess. (Mo. 2009) (enacted)	<p>Any person that owns or licenses personal information of residents of Missouri or any person that conducts business in Missouri that owns or licenses personal information in any form of a resident of Missouri shall provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach.</p> <p>Breach of security is an unauthorized access to and an unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. Good faith acquisition of personal information by</p>	<p>Notice must be made (a) without unreasonable delay; (b) consistent with the needs of law enforcement; and (c) consistent with any measures necessary to determine sufficient contact information and to determine the scope of the breach and restore the reasonably integrity, security, and confidentiality of the data system.</p> <p>Notice may be delayed by law enforcement.</p> <p>In the event a person provides notice to more than 1000 consumers at one time the person shall notify, without unreasonable delay,</p>	<p>At a minimum, the notice shall include a description of the following: (a) the incident in general terms; (b) the type of personal information obtained as a result of the breach of security; (c) a telephone number the affected consumer may call for further information and assistance, if one exists; (d) contact information for consumer reporting agencies; (e) advice directing the affected consumer to remain vigilant by reviewing account statements and monitoring free credit reports.</p> <p>Regular notice shall be provided by one of the following methods: (a) written notice; (b) electronic notice to</p>	<p>Any person that maintains or possesses records or data containing personal information of residents of Missouri that the person does not own or license, or any person that conducts business in Missouri that maintains or possesses records or data containing personal information of a resident of Missouri that the person does not own or license, shall notify the owner or licensee of the information of any breach of security immediately following discovery of the breach, consistent with the</p>	<p>A person that maintains its own notice procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements, is deemed to be in compliance with the notice requirements if the person notifies affected consumers in accordance with its policies in the event of a breach of security of the system.</p>	<p>No notice required if, after appropriate investigation by the person or after consultation with the relevant responsible law enforcement agency, the person determines that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach. This determination must be documented in writing and maintained for five years.</p>	<p>The attorney general has the exclusive authority to bring an action to obtain actual damages for a willful and knowing violation of this section and may seek a civil penalty not to exceed \$150,00 per breach of the security of the system or series of breaches of a similar nature that are discovered in a single investigation.</p>	<p>A person that is regulated by state or federal law and that maintains procedures for a breach of the security of the system under the laws, rules, regulations, guidance, or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance if the person notifies affected consumers in accordance with the maintained procedures when a breach occurs.</p> <p>A financial institution that is: (a) subject to and in compliance with the Federal Interagency</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>a person or that person's employee or agent for a legitimate purpose of that person is not a breach of security, provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the personal information.</p> <p>Personal information is an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the</p>	<p>the attorney general's office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. Section 1681a(p), of the timing, distribution, and content of the notice.</p>	<p>consumers with a valid email address and who have agreed to receive electronic communications (if it is consistent with federal electronic signature laws); (c) telephonic notice, if contact is made directly with the affected consumers.</p> <p>Substitute notice is possible if (a) person demonstrates that the costs of providing notice would exceed \$100,000; (b) the class of affected consumers exceeds 150,000; (c) the person does not have sufficient contact information or consent to satisfy regular notice for those affected consumers without sufficient contact information or consent; or (d) the person is unable to identify</p>	<p>legitimate needs of law enforcement.</p>				<p>Guidance Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued on March 29, 2005, by the board of governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, and any revisions, additions, or substitutions relating to said interagency guidance; or (b) subject to and in compliance with the National Credit Union Administration regulations in 12 CFR Part 748; or (c)</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	name or data elements are unreadable or unusable: (a) SSN; (b) driver's license number or other unique identification number created or collected by a government body; (c) financial 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 an individual's financial account; (d) unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (e) medical information; or (f) health insurance information.		particular affected consumers, for only those unidentifiable consumers. Substitute notice must consist of all of the following: (a) email notice when the person has an email address for the affected consumer; (b) conspicuous posting of the notice or a link to the notice on the website of the person if the person maintains a website; and (c) notification to major statewide media.					subject to and in compliance with the provisions of GLB shall be deemed to be in compliance.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	Personal information does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public;							
Montana Mont. Code Ann. § 30-14-1704	Any business that owns or leases computerized data and conducts business in Montana must disclose a breach of a security system if it reasonably believes there has been an unauthorized acquisition of unencrypted information. A breach of a security system is an unauthorized acquisition of computerized data that	Notice may be delayed to assist with law enforcement, but must be provided after law enforcement determines it will not compromise investigation. Notice must be consistent with measures necessary to determine the scope of the breach and restore reasonable integrity of the system.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws); 3) telephonic notice; or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds	Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of any breach following discovery of the breach if the Personal Information may have been acquired by an unauthorized person.	A business that maintains its own notification procedures can use its own policy as long as the policy does not unreasonably delay notice to consumers.		Certain government agencies are authorized to bring enforcement actions in the public interest.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>compromises the security, confidentiality or integrity of Personal Information and causes or is reasonably believed to cause loss or injury to a Montana resident.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number, MT identification card number or trial identification card; or (3) account number or credit/debit card number with any required security code, access code or password.</p>		<p>500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p> <p>If notice provided under this law suggests or implies that a consumer can obtain a copy of their file from the CRA the business must coordinate with the CRA regarding the timing, content, and distribution of notice to the Montana consumer as long as the cooperation cannot unreasonably delay the notice.</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
			Notice content required.					
Nebraska Neb. Rev. Stat. §§ 87-801 to -806	Any individual or commercial entity that (i) conducts business in Nebraska; and (ii) owns or licenses computerized data that includes Personal Information about a Nebraska resident, must provide notice of a security breach of their system if it is determined that the use of information has occurred or is about to occur. Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or state identification	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed by law enforcement agencies.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws); 3) telephonic notice; or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$75,000; (ii) the effected class exceeds 100,000 persons; or (iii) insufficient contact information. Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is	Persons that maintain computerized data owned by others that includes Personal Information must give notice to and cooperate with the owner or licensee of the information of any breach following discovery of the breach if use of the Personal Information has occurred or is reasonably likely to occur.	If a person maintains a notification procedures as part of its information security policy for Personal Information, it may be utilized if it is otherwise consistent with the timing requirements of this law.		The Attorney General may bring enforcement actions.	A data owner who is regulated by state or federal law and who maintains procedures for breaches pursuant to the laws, rules, regulations, guidance or guidelines established by the applicable principal regulator is deemed to be in compliance with this statute if the entity complies with the maintained procedures.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	card number; (3) account number or credit/debit card number with any required security code, access code or password; (4) unique electronic identification number or routing code, in combination with any required security code, access code or password; or (5) unique biometric data (fingerprint, voice print, or retina or iris image or other unique physical representation). PI definition includes biometric data.		maintained); and (c) notification to major statewide media. If the individual has 10 or fewer employees and the cost of providing notice will exceed \$10,000, substitute notice is also available, which must be provided as set forth above and with the additional requirement that notice be set forth in a paid advertisement in a local newspaper (at least ¼ page) in the geographic area once a week for three weeks.					
Nevada Nev. Rev. Stat § 603A	Any business that owns or licenses computerized data that includes Personal Information of Nevada residents must disclose a breach of a security system to such person if	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws); or	Persons that maintain computerized data owned by others that includes Personal Information must give notice to the	If a person maintains a notification procedures as part of its information security policy for Personal Information, it may		The Attorney General may bring actions for injunctive relief for violations. Data collectors who provide	A data collector who is subject to and complies with the security provisions of GLB is deemed to be in compliance.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>it is determined that such person's Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>If notification is to more than 1,000 persons at one time, the person giving notice shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.</p> <p>A breach of a security system is an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of Personal Information.</p> <p>Personal Information means an individual's first name or first initial and last name in</p>	<p>legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system.</p> <p>Notice can be delayed if instructed by law enforcement agencies.</p>	<p>3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>owner or licensee of the information of any breach following discovery of the breach if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>be utilized if it is otherwise consistent with the timing requirements of this law.</p>		<p>timely notice may bring actions for damages against a person that unlawfully obtained or benefited from Personal Information maintained by the data collector. Damages, costs of the action, attorneys' fees, costs of notification as well as punitive damages are recoverable.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or NV identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p> <p>Notice to other entities required.</p>							
New Hampshire N.H. Rev. Stat. Ann. §§ 359-C:19 to -C:21	Any agency, individual or commercial entity that conducts business in New Hampshire that owns or licenses computerized data that includes Personal Information about a New Hampshire resident must give notice to the affected resident if it becomes aware of a breach of the security of the system	Notice must be given as soon as possible, but may be delayed by a law enforcement agency.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it is the primary means of communication with affected individual); 3) telephonic notice (provided a log is kept); or 4) substitute notice.	Persons that maintain computer data that it does not own or license that includes Personal Information must notify the owner or licensee of the Personal Information if the Personal Information was, acquired by an unauthorized			Any person injured may bring an action for damages and for equitable relief. If the act was a willful or knowing violation, it shall award as much as 3 times, but not less than 2 times, this amount. The prevailing party is	Any person engaged in trade or commerce which maintains procedures for security breach notifications pursuant to the laws, rules and regulations issued by the applicable federal or state regulator are deemed to be in

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>and determines the misuse has occurred or is reasonably likely to occur. Notice is also required if the person cannot determine if the misuse of information has occurred or is reasonably likely to occur.</p> <p>If notification is to more than 1,000 persons at one time, the person giving notice shall also notify all consumer reporting agencies of the anticipated date of the notification to the consumers, the appropriate number of consumers who will be notified and the content of the notification.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of</p>		<p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$5,000; (ii) the effected class exceeds 1,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p> <p>Notice must include: 1) a description of the incident in general terms; 2) the approximate date of the breach; 3) the type of Personal Information obtained; and</p>	person.			also to be awarded costs of the suit and reasonable attorneys' fees.	compliance.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>the following when the data element is not encrypted: (1) SSN; (2) driver's license number or government identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p> <p>Notice to Other Entities is Required.</p>		<p>4) telephonic contact information of the person whose system was breached.</p> <p>Notice content required.</p>					
New Jersey N.J. Stat. Ann. §§ 56:8-161, -163	Any entity that conducts business in New Jersey that owns or licenses computerized data that includes Personal Information of New Jersey residents must disclose a breach of a security system to such person if it is determined that such person's Personal Information was, or is reasonably believed to have been, acquired by	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the	<p>Disclosure to be given in one of the following forms:</p> <p>1) written notice; 2) electronic notice (if it is consistent with federal electronic signature laws); or 3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the</p>	Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of any breach following discovery of the breach if the Personal Information was, or	If a person maintains a notification procedures as part of its information security policy for Personal Information, it may be utilized if it is otherwise consistent with the timing requirements of this law.	Disclosures not required if the entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and maintained for five years.	A knowing or reckless violation of this law is an unlawful business practice in New Jersey.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>an unauthorized person.</p> <p>A breach of a security means unauthorized access to electronic files, media or data containing Personal Information a that compromises the security, confidentiality or integrity of Personal Information when access to the Personal Information has not been secured by encryption or by any other method or technology that renders the Personal Information unreadable or unusable.</p> <p>If notification is to more than 1,000 persons at one time, the person giving notice shall also notify all consumer reporting agencies that compile and maintain files on consumers on a</p>	<p>reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed by law enforcement agencies.</p> <p>Notice must also be provided (in advance of disclosure to the consumer) to the Division of State Police in the Department of Law and Public Safety for investigation or handling.</p>	<p>effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>is reasonably believed to have been, acquired by an unauthorized person.</p>				

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>nationwide basis.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following data element: (1) SSN; (2) driver's license number or government identification card number; or (3) account number or credit/debit card number with any required security code, access code or password. Dissociated data that, if linked, would constitute Personal Information if the means to link the dissociated data were accessed in connection with access to the dissociated data.</p> <p>Notice to Other Entities is Required.</p>	<p>State Police must be notified before consumers are notified.</p>						

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
New York N.Y. Gen. Bus. Law § 899-aa	Any entity that conducts business in New York that owns or licenses computerized data that includes Personal Information of New York residents must disclose a breach of a security system to such person if it is determined that such person's Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person. If more than 5,000 New York residents are to be notified at one time, the consumer reporting agencies must also be notified as to the timing, content and distribution the notices and approximate number of affected persons. This notice must be made without delaying notice to affected New York	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed by law enforcement agencies.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if consent is provided and a log is kept); 3) telephonic notice; or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information. Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.	Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of any breach following discovery of the breach if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.			Actions may be brought by the Attorney General. Injunctive relief and consequential damages (including reasonable attorneys' fees) are recoverable. Civil Penalties are the greater of \$5,000 or \$10 per failed notice, but not to exceed \$150,000.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>residents.</p> <p>A breach of a security system is an unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of Personal Information.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following data element: (1) SSN; (2) driver's license number or government identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p>		<p>Notice must provide contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of Personal Information and private information were, or are reasonably believed to have been, acquired.</p> <p>Notice must also be provided to the State Attorney General, the Consumer Protection Board, the State Office of Cyber Security and Critical Infrastructure Coordination Board as</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	Notice to other entities required.		to the timing, content and distribution of the notice and the approximate number of affected persons. Notice content required.					
New York City N.Y. City Admin. Code § 20-117	Any business subject to the jurisdiction of the Department of Consumer Affairs that also owns, leases or maintains data that includes Personal Information must disclose to the Department of Consumer Affairs and to the police department any breach of security if it is reasonably believed to have been acquired by an unauthorized person. Notice must also be provided to the residents.	As soon as practicable by a method reasonable under circumstances, provided that the timing is not inconsistent with the legitimate needs of law enforcement or any other investigate or protective measures necessary to restore the reasonable integrity of the system.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice; or 3) substitute notice if either of the above is impracticable. If impracticable, then by a mechanism chosen by the licensee that is reasonably targeted to the individual.	Entities that maintain data must give notice of the breach to the owner of the data.			Punishable by a fine of not more than \$500 and a person or entity that violates this law is liable for a civil penalty of \$100 for each violation.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>Personal Information is any person's date of birth, SSN, drivers license number, non-driver photo identification card, financial services account (bank, credit card, debit card, broker account, ATM, etc.) number or code, mother's maiden name, computer system password, electronic signature or unique biometric data that is a fingerprint, voice print, retinal image or iris image of another person.</p> <p>PI definition includes biometric data.</p> <p>Notice to other entities required and the law may cover all forms of data..</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
North Carolina N.C. Gen. Stat. §§ 75-61, -65	<p>Any business that owns or licenses computerized data that includes North Carolina resident's Personal Information, or any business that conducts business in North Carolina that owns or licenses Personal Information in any form must provide notice to the affected person of a breach.</p> <p>If notice is given to more than 1,000 persons at one time, the business must also notify the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile data on a nationwide basis.</p> <p>Personal information means a person's first name or first initial and</p>	Must be made without unreasonable delay, consistent with the legitimate needs of law enforcement, with any measures necessary to determine sufficient contact information, and to determine the scope of the breach and restore the reasonable integrity of the system.	<p>Disclosure to be given in one of the following forms:</p> <ol style="list-style-type: none"> 1) written notice; 2) electronic notice (if consented to); 3) telephonic notice (provided a log is kept); or 4) substitute notice. <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of any breach following discovery of the breach if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.			The law does not create a private right of action, unless the person is actually injured. Violation of this law is a violation of § 75-1.1.	Entities in compliance with the Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Consumer Notice, are governed by the Board of Governors of the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency and the Office of Thrift Supervision are deemed to be in compliance.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	last name in combination with any of the following identifying information: (1) SSN or employer taxpayer ID number; (2) drivers license, State identification card, or passport numbers; (3) checking account numbers; (4) savings account numbers; (5) credit card numbers; (6) debit card numbers; (7) personal identification code; (8) electronic identification numbers, electronic mail names or addresses, internet account numbers, or internet identification names; (9) digital signatures; (10) any other numbers or information that can be used to access a person's financial resources; (11) biometric data; (12) fingerprints; (13)		<p>Notice must include a description of the following:</p> <p>1) the incident in general terms;</p> <p>2) the type of Personal Information subject to breach;</p> <p>3) general acts of the business to protect information from further breaches;</p> <p>4) a telephone number that a person may call for further information; and</p> <p>5) advice that directs the person to remain vigilant in reviewing account statements and monitoring free credit reports.</p> <p>Notice content required.</p> <p>2009 N.C. Sess. Laws page no. 355 (amending N.C. Gen.</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>passwords; or (14) parent's legal surname prior to marriage.</p> <p>Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records.</p> <p>Personal Information DOES NOT include electronic identification numbers, electronic mail names or addresses, Internet account numbers,</p>		<p>Stat. § 75-65), effective October 1, 2009:</p> <p>Notice must include all of the following:</p> <ol style="list-style-type: none"> 1) a description of the incident in general terms; 2) a description of the type of Personal Information subject to breach; 3) a description of the general acts of the business to protect information from further breaches; 4) a telephone number for the business that a person may call for further information; 5) advice that directs the person to remain vigilant in reviewing account statements and monitoring free credit reports; 6) the toll-free numbers and addresses for the major consumer 					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>Internet identification names, parent's legal surname prior to marriage, or a password unless this information would permit access to a person's financial account or resources.</p> <p>Notice to Other Entities is Required.</p> <p>Disclosure includes all forms of data, including paper.</p>		<p>reporting agencies; and 7) the toll-free numbers, addresses, and website addresses for the Federal Trade Commission and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from these sources about preventing identity theft.</p> <p>In the event a business provides notice to an affected person under this section, the business shall notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office of the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
			prevent a similar breach in the future, and information regarding the timing, distribution, and content of the notice.					
North Dakota N.D. Cent. Code §§ 51-30-01 to -07	Any business that owns or licenses computerized data that includes Personal Information of North Dakota residents must disclose a breach of a security system to such person if it is determined that such person's Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person. A breach of a security system is an unauthorized acquisition when access to Personal Information has not been secured by encryption that renders	Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed by law enforcement agencies.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if it complies with electronic signature); or 3) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information. Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting	A licensor of personal data must also give notice to the owner of the data if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.	If a person maintains a notification procedures as part of its information security policy for Personal Information, it may be utilized if it is otherwise consistent with the timing requirements of this law.		The Attorney General may bring enforcement actions.	A financial institution, trust company or credit unit that is subject to, examined for and in compliance with the federal interagency guidance on response programs for unauthorized access to customer information and customer notice is deemed to be in compliance with North Dakota law.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>the files, media or data bases unreadable or unusable.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or North Dakota identification card number; (3) account number or credit/debit card number with any required security code, access code or password; (4) the individual's date of birth; (5) the maiden name of the individual's mother; (7) an identification number assigned to the individual by the individual's employer; or (8) the individual's</p>		<p>on website (if one is maintained); and (c) notification to major statewide media.</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	digitized or other electronic signature. PI definition includes electronic signatures and other electronic identifiers.							
Ohio Ohio Rev. Code Ann. § 1349.19	Any business that owns or licenses computerized data that includes Personal Information of Ohio residents must disclose a breach of a security system to such person if it is determined that such person's Personal Information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person if the access and acquisition causes or is reasonably believed to cause a material risk of identity theft or other fraud. If notice is given to	Notice to be provided in most expedient time possible but no later than 45 days following discovery, subject to the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach, including which residents' Personal Information was accessed and acquired.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if consented to); 3) telephonic notice; or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information. Substitute notice must consist of: (a) email notice (if email	A licensor of personal data must also give notice to the owner of the data if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, if it is reasonably believed the acquisition will cause a material risk of identity theft or other fraud to a resident of Ohio.			The Attorney General may bring enforcement actions.	Financial institutions, trust companies, credit unions that are required by federal law to notify its customers of an information security breach is exempt from compliance.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>more than 1,000 persons at one time, the business must also notify the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile data on a nationwide basis.</p> <p>A breach of the security of the system means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of Personal Information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft.</p> <p>Personal Information means an individual's</p>		<p>addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p> <p>Substitute notice is also permitted if the person giving notice is a business with 10 or fewer employees and costs will exceed \$10,000, in which case the notice will consist of a paid advertisement in a local newspaper distributed in the geographic area at least once a week for three consecutive weeks, posting on the businesses website and notification to major media outlets in the area.</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (1) SSN; (2) driver's license number or state identification card number; or (3) account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.</p> <p>Notice to Other Entities is Required.</p>	<p>Notice in 45 days</p>						

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Oklahoma Okla. Stat. tit. 24, §§ 161 to 166 (Effective November 2008)	An individual or entity that owns or licenses computerized information that includes Personal Information of Oklahoma residents must disclose any breach of the security of such a system to that person if that person's unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and that access has caused or it is believed will cause identity theft or fraud. The disclosure of encrypted personal information must be disclosed if the information is acquired and accessed in unencrypted form	The disclosure must be made without unreasonable delay consistent with the need to take any measure to determine the scope of the breach and to restore the reasonable integrity of the system. Notice may be delayed if a law enforcement agency determines and advises the individual or entity that notice will impede a criminal or civil investigation or homeland or national security.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if consented to); 3) telephonic notice; or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$50,000; (ii) the effected class exceeds 100,000 persons; or (iii) insufficient contact information. Substitute notice must consist of any two of the following : (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.	An entity that maintains data that includes personal information must notify the owner or licensee of the information of any breach of security as soon as practical if it is believed that personal information was accessed and acquired by an unauthorized person.	An entity that maintains its own notification procedures as part of an information privacy or security policy for the treatment of information that is consistent with the timing requirements of this law is deemed to be in compliance with the notification requirements of the law if it provides notice in a manner consistent with the law in the event of a security breach.		There is no private right or action. Instead, a violation of the law may be enforced by the Attorney General or a district attorney as an unlawful practice under the Oklahoma Consumer Protection Act. Actual damages resulting from a violation of the act or a civil penalty not to exceed \$150,000 per breach of the security of the systems or series of breaches of a similar nature that are discovered in a single investigation.	A financial institution that complies with the notification requirements prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be compliance with this law. An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator of the

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>during a security breach or if the breach was accomplished by someone with access to a encryption key and the individual or entity believes that such breach has or will cause identity theft or fraud.</p> <p>Personal information includes information the unencrypted or unredacted first name or first initial and last name of a person in combination with: (1) SSN; (2) driver's license or identification number; (3) financial account number or credit credit/debit card number in combination with any required security code, access code or password.</p>						Violations of the act by state chartered or state licensed financial institutions may only be enforced by the primary state regulator of the institution.	entity shall be deemed to be in compliance with the law.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Oregon Or. Rev. Stat. §§ 646A.602 to .604	<p>Any person that owns or licenses information that includes Personal Information of Oregon residents must disclose a breach of a security system to such person.</p> <p>If notice is given to more than 1,000 persons at one time, the business must also notify the Consumer Protection Division of the Attorney General's Office and all consumer reporting agencies that compile data on a nationwide basis.</p> <p>Personal Information means a consumer's first name or first initial and last name in combination with any one or more of the following data elements, when the data elements are not rendered unusable through</p>	Disclosure must be made in the most expeditious time possible and without unreasonable delay, consistent with legitimate needs of law enforcement, and consistent with any measures necessary to determine sufficient contact information for the consumers, determine the scope of the breach and restore the reasonable integrity.	<p>Disclosure to be given in one of the following forms:</p> <p>1) written notice; 2) electronic notice (if consented to); 3) telephonic notice (if given directly); or 4) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 350,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	A licensor of personal data must also give notice to the owner of the data of the occurrence of any breach of security if Personal Information was included in the breach.		No notice is required if, after investigation and consultation with authorities, the person determines there is no reasonable likelihood of harm to the person whose information was acquired. Documentation must be maintained for 5 years if no notice is provided.		Law does not apply to a person with notification requirements or breach of security procedures that provide greater protection to Personal Information and at least as through disclosure requirements pursuant to the rules, regulations, procedures, guidance or guidelines established by the person's primary or functional federal regulator; a person that complies with a state or federal law that provides greater protection to Personal Information and at least as thorough disclosure requirements for a breach of security of

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	encryption, redaction or other methods, or when the data elements are encrypted and the encryption key has also been acquired: (1) SSN; (2) driver license number or state identification card number issued by the Department of Transportation; (3) passport number or other United States issued identification number; or (4) financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account. It also means any of the data elements or any combination of these data elements when not combined with the		A notice must contain at a minimum: (1) a description of the incident in general terms; (2) the approximate date of the breach; (3) type of personal information obtained; (4) contact information of a person subject to the law; (5) contact information for national consumer reporting agencies; (6) advice to the consumer concerning the reporting of identity theft.					Personal Information than that provided by this law; or a person that complies with GLB.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>consumer's first name or first initial and last name and when the data elements are not rendered unusable through encryption, redaction or other methods, if the information obtained would be sufficient to permit a person to commit identity theft against the consumer whose information was compromised. It does not include information, other than a Social Security number, in a federal, state or local government record that is lawfully made available to the public.</p> <p>Redacted means altered or truncated so that no more than the last four digits of a Social Security number, driver license number, state identification card</p>							

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>number, account number or credit or debit card number is accessible as part of the data.</p> <p>Encryption means the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key.</p> <p>Notice to Other Entities is Required.</p>		Notice content required.					
<p>Pennsylvania</p> <p>73 Pa. Stat. Ann. §§ 2301 to 2329</p>	<p>Any business that owns or licenses computerized data that includes Personal Information of Pennsylvania residents must disclose a breach of a security system to such person if it is determined that such person's Personal</p>	<p>Notice may be delayed at the request of law enforcement.</p>	<p>Disclosure to be given in one of the following forms:</p> <p>1) written notice;</p> <p>2) electronic notice (if a prior business relationship exists and the person or entity has a valid email address for the individual); or</p> <p>3) telephonic notice (if</p>	<p>A licensor of personal data must also give notice to the owner of the data if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>An entity that maintains its own notification procedures that is consistent with the notice requirements are deemed to be in compliance.</p>		<p>Violations are an unfair or deceptive act or practice in violation of the act of the Unfair Trade Practices and Consumer Protection Law.</p>	<p>A financial institution that complies with the notification requirements prescribed by Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>Information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.</p> <p>Encryption alone does not necessarily obviate the need for notice. An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.</p> <p>If notice is given to more than 1,000 persons at one time, the business must also notify all consumer reporting agencies that</p>		<p>the customer can reasonably be expected to receive it and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies Personal Information but does not require the customer to provide Personal Information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance); or</p> <p>4) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$100,000; (ii) the effected class exceeds 175,000 persons; or (iii) insufficient contact information.</p>					<p>Information and Customer Notice is deemed to be in compliance with the law.</p> <p>An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines, established by the entity's primary or functional Federal regulator will be in compliance with the act.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>compile and maintain files on consumers on a nationwide basis.</p> <p>A breach is the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of Personal Information maintained by the entity and that causes or reasonably believes has or will cause the loss or injury to any residents.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or PA identification card number; (3) account number or credit/debit</p>		<p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	card number with any required security code, access code or password. Notice to Other Entities is Required.							
Puerto Rico P.R. Laws Ann. tit. 10, §§ 4051 to 4055	Owners or custodians of commercial databases which contain a Personal Information archive of citizens residing in Puerto Rico must notify those citizens of a security breach if the database contains a personal information archive that is not protected with a crypto-graphical code beyond a password. Personal information archive is a file containing at least a name or first initial and the last name of a person, combined with any of the following data	Notification to clients must be performed in the most expedited manner considering the need of public order agencies to maintain crime scenes and evidence and the need to reinstate Security.	Disclosure to be given in one of the following forms: (1) Written Notice; (2) Electronic Mail or Electronic Media pursuant to the Digital Signature Act; (3) Substitute notice. Substitute notice is permissible only if: (i) the costs of the other forms of notice is too expensive due to the amount of effected individuals, the difficulty of locating all effected individuals, the economic situation of the company or entity;	All entities that resell or provide access to digital databases which contain personal information archives of citizens must notify the owner, custodian or holder of the information of any security breach of the system that allowed access by unauthorized persons.			The Secretary may impose fines from \$500 to \$5,000 for each violation of the law. These fines do not preclude a consumer from suing for damages.	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>without the need to use a special cryptographic code to access it: (1) SSN; (2) Driver's license number, electoral card, or an official identification; (3) banking or financial account numbers with or without the password; (4) name of users and passwords to public or private computer systems; (5) Medical information protected by HIPAA; (6) tax information; (7) labor evaluations.</p> <p>The party must inform the Department of Consumer Affairs within 10 days after a breach of the security system is detected. The Department is required to make a public announcement within the next working day of receiving the</p>		<p>or</p> <p>(ii) the costs of providing notices exceeds \$100,000; (iii) or the number of effected individuals exceeds 100,000.</p> <p>Substitute notice can be made through: (1) prominent posting on the entity's website; (2) inside any brochure published and sent through postal or electronic mail; (3) or through a press release that gives information concerning the situation and contact information. If the information is relevant in a specific commercial or professional sector, the ad must be published through publication or programming targeted</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>information.</p> <p>Notice to Other Entities Is Required</p> <p>PI definition includes health, health insurance, tax and certain employment data.</p> <p>Could be read to include non-computerized data, though it may only apply to computerized data.</p>		<p>to the biggest circulation sector.</p> <p>Notice must include, as far as possible:</p> <p>(1) needs of any current investigation or court case; (2) nature of the situation; (3) number of clients affected; (4) if criminal complaints have been filed; (5) what measures are being taken and an estimate of cost and time to rectify the situation; and (6) if it known how the information was breached the right to know which information was compromised.</p> <p>Notice content required.</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Rhode Island R.I. Gen. Laws §§ 11-49.2-1 to -7	<p>Any person that owns or licenses computerized data that includes Personal Information of Rhode Island residents must disclose a breach of a security system to such person if it is determined that such person's Personal Information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.</p> <p>A breach is the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of Personal Information maintained by the entity.</p> <p>Personal Information means an individual's first name or first initial</p>	<p>Notification must be prompt and reasonable following determination of the breach.</p> <p>Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system.</p> <p>Notice can be delayed if instructed by law enforcement agencies.</p>	<p>Disclosure to be given in one of the following forms:</p> <ol style="list-style-type: none"> 1) written notice; 2) electronic notice (if consistent with federal law); or 3) substitute notice. <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$25,000; (ii) the effected class exceeds 50,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of any breach immediately following discovery of such breach if such breach poses a significant risk of identity theft and the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>If a person maintains a notification procedures as part of its information security policy for Personal Information, it may be utilized if it is otherwise consistent with the timing requirements of this law.</p>	<p>Notification is not required if, after an appropriate investigation or after consultation with relevant authorities, a determination is made that the breach has not and will not likely result in a significant risk of identity theft.</p>	<p>Each violation is a civil violation for which a penalty of not more than \$100 per occurrence and not more than \$25,000 may be granted against a defendant.</p>	<p>A person that maintains a security policy that complies with GLB, HIPAA or certain other federal requirements is deemed to be in compliance.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or RI identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.							
South Carolina S.C. Code Ann. § 39-1-90 (Effective July, 2009)	A person that conducts business in South Carolina that owns or licenses computerized information containing Personal Identifying Information must disclose a breach of security to a resident of South Carolina whose information that not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to	Notice of the breach must be provided in the most expedient time possible and within the most expedient time. This notification may be delayed if a law enforcement agency determines that the notice impedes a criminal investigation.	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if the primary method of communication or is consistent with federal law); or 3) telephone notice; or 4) substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed	A person that conducts business in South Carolina and that maintains computerized data which includes personal identifying information must notify the owner or licensee of the information immediately upon discovery of a security breach.	A person that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information that is otherwise consistent with the timing requirements of this law is considered to be in compliance with		The Department of Consumer affairs may impose a fine in the amount of \$1,000 for each resident whose information was accessed by the breach in the case of a willful and knowing violation of the statute. A resident of	This law does not apply to bank or other financial institution that is subject to and in compliance with the GLB. A institution that is in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>have been, acquired by unauthorized person, when illegal use of information has occurred or reasonably likely to occur or use of the information creates a material risk of harm to the resident.</p> <p>Personal Identifying Information is defined in SC Code Ann. § 16-13-501. SC Code 16-13-501 currently lists specific types of identifying information however an amendment currently passed by the South Carolina Senate amends the statute to define personal information consistent with other states. The amendment defines personal identifying information as: the first name or first initial and last name in combination with</p>		<p>\$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>		<p>the law if the person notifies subject persons in accordance with its policies.</p>		<p>South Carolina injured by a willful and knowing violation of this act may bring an action for actual damages resulting from a negligent violation of the law saw, seek an injunction to enforce compliance, and may recover attorneys fees.</p> <p>Treble damages are available for willful violations of the act not to exceed \$1,000 for each incident.</p> <p>If the injury is to the consumers credit capacity, character, general</p>	<p>Information and Customer Notice, issued March 7, 2005, by the board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision is considered to be in compliance with this law.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>unencrypted or unredacted (1) SSN; (2) driver's license number or identification number; (3) financial account number, credit/debit card number in combination with a security code, access code, or password that permits access to the account; (4) other numbers or information that may be used to access the account or numbers or information issued by a governmental or regulatory agency entity that uniquely identifies an individual (Amended by 2008 South Carolina Laws Act 190 (S.B. 453).</p> <p>If a business provides notice to more than 1,000 person at one, under this law, the business must notify</p>						<p>reputation, employment options, or eligibility for insurance, and results from the failure to enforce a security freeze and the failure is not corrected by the consumer credit reporting agency within 10 days after then entry of judgment of damages, the assessed damages must be increased to not more than \$1,000 each day until the security fee is imposed.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>without unreasonable delay, the Consumer Protection Division and all consumer reporting agencies that compile and maintain files on a nationwide basis.</p> <p>Notice to other entities required.</p> <p>Amendment was effective July 1, 2009.</p> <p>Applies to computerized and "other data".</p>							
Tennessee Tenn. Code Ann. § 47-18-2107	<p>Breaches of security must be disclosed following discovery or notification of the breach to any Tennessee resident whose unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the</p>	<p>Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if consistent with federal law); or 3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed</p>	<p>Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of any breach immediately following discovery</p>	<p>If a person maintains notification procedures as part of its information security policy for Personal Information, it may be utilized if it is otherwise consistent with the timing requirements of</p>		<p>Residents injured by a violation may recover damages, as well as injunctive relief, to enjoin from further actions in violation of law.</p>	<p>Does not apply to persons who are subject to the provisions of GLB.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>If notice is given to more than 1,000 persons at one time, the business must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number; or (3) account number or credit/debit card number with any required security code, access code or password.</p> <p>Notice to Other Entities is Required.</p>	<p>scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed by law enforcement agencies.</p>	<p>\$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>of such breach if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>this law.</p>			

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Texas Tex. Bus. & Com. Code Ann. § 521.053	<p>Any person that owns or licenses computerized data that includes sensitive Personal Information of Texas residents must disclose a breach of a security system to such person if it is determined that such person's sensitive Personal Information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.</p> <p>If notice is given to more than 10,000 persons at one time, the business must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.</p> <p>Personal Information means an individual's</p>	<p>Notice should be made as quickly as possible, though it may be delayed if instructed by law enforcement agencies.</p>	<p>Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if consistent with federal law); or 3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); OR (c) notification to major statewide media.</p>	<p>Any person that maintains computerized data that includes sensitive Personal Information that the person does not own must notify the owner or license holder of the information of any breach immediately after discovering the breach, if the sensitive Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>If a person maintains notification procedures as part of its information security policy for Personal Information, it may be utilized if it is otherwise consistent with the timing requirements of this law.</p>		<p>Violations are punishable by not less than \$2,000 but not more than \$50,000 for each violation. The attorney general may bring suits to recover damages.</p> <p>Injunctive relief and attorneys' fees may also be obtained.</p> <p>Other equitable relief may be granted by the court, in its discretion.</p> <p>A violation of this law is also considered to be a deceptive trade practice under Section 48.101 of the Texas Business and</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>first name or first initial and last name in combination with (A) any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number; or (3) account number or credit/debit card number with any required security code, access code or password or (B) information that identifies an individual and relates to physical or mental health or payment for the provision of health care to the individual.</p> <p>"Breach of system security" means "unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity ... including data that is encrypted if the person accessing the</p>						<p>Commercial Code.</p> <p>Victims of identity theft may seek a declaration from the Texas courts that they were victims of identity theft.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p><i>data has the key required to decrypt the data."</i></p> <p><i>Italics effective Sept. 1, 2009.</i></p> <p>Notice to Other Entities is Required.</p>							
Utah Utah Code Ann. §§ 13-44-101 to -301	<p>Any person that owns or licenses computerized data that includes Personal Information concerning a Utah resident must, after becoming aware of a breach, conduct a good faith investigation to determine the likelihood that Personal Information has been or will be misused for identity fraud or a theft or fraud purpose, provide notice to all affected Utah residents.</p> <p>A breach is the unauthorized access and acquisition of</p>	<p>Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed</p>	<p>Notice must be given in writing by first-class mail, electronically if that is the primary method of communication with the person (if it complies with federal law), by telephone, including through the use of automatic dialing systems, or by publishing notice in a newspaper of general circulation.</p>	<p>Any person that maintains Personal Information must give notice to the person that owns the information immediately following discovery of a breach, if misuse of Personal Information is likely to occur.</p>	<p>Existing security policies that include notice in the event of a security breach can be followed if they are otherwise consistent with this law and compliance with any federal law requiring notice is in compliance with this statute.</p>		<p>Law does not create a private right of action. Civil penalties of \$2,500 per violation or series of violations, up to \$100,000 in the aggregate are available.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>computerized data that materially compromises the security or confidentiality of Personal Information maintained by the entity.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number; or (3) account number or credit/debit card number with any required security code, access code or password.</p>	by law enforcement agencies.						
Vermont Vt. Stat. Ann. tit. 9, §§ 2430 to 2435	Any person that owns or licenses computerized Personal Information that includes Personal Information concerning a Vermont resident shall	Notification of breach must be provided in the most expedient time possible and without	Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice; 3) telephonic notice; or	Any person that maintains computerized data that includes Personal Information that the		Notice is not required if it can be established that misuses of Personal Information is not	Attorney General and State Attorney have enforcement power.	A financial institution that is subject to the following guidances, and any revisions, additions, or

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>notify the consumer that there has been a breach of security.</p> <p>If notice is given to more than 1,000 persons at one time, the business must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.</p> <p>A breach is the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of Personal Information maintained by the entity.</p> <p>Personal Information means an individual's first name or first initial and last name in</p>	<p>unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity, security and confidentiality of the system. Notice can be delayed if instructed by law enforcement agencies.</p>	<p>4) substitute notice.</p> <p>Electronic notice is only permissible if a valid email address exists and the person does not have certain contact information and email is the primary means of communication between the parties, the notice does not include a hypertext link to a request that Personal Information be provided and the notice conspicuously warns consumers not to provide Personal Information in response to the communication.</p> <p>Telephonic notice must be direct (i.e. no prerecorded messages).</p>	<p>person does not own must notify the owner or license holder of the information of any breach immediately after discovering the breach. Notification may be delayed at the request of law enforcement.</p>		<p>possible and notice of such determination is Vermont attorney general or the department of banking, insurance, securities and health care administration in the event that they are licensed in Vermont.</p>		<p>substitutions relating to the following interagency guidance is exempt from this law: The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision; or Final Guidance on Response Programs for Unauthorized Access to Member Information and</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number; (3) account number or credit/debit card number if they can be used without any access codes; or (4) account passwords or personal identification numbers or other access codes for a financial account.</p> <p>Notice to Other Entities is Required.</p>		<p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$5,000; (ii) the effected class exceeds 5,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); OR (c) notification to major statewide media.</p> <p>Notification must include a description of the following: 1) the incident in general terms; 2) the type of Personal Information subject to</p>					Member Notice, issued on April 14, 2005, by the National Credit Union Administration

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
			<p>access or acquisition; 3) the general acts of the business to protect the Personal Information from further unauthorized access or acquisition; 4) a toll-free number that the consumer may call for further information and assistance; and 5) advice that directs the consumer to remain vigilant by reviewing account information and monitoring credit reports.</p> <p>Notice content required.</p>					
Virginia Va. Code. Ann. § 18.2-186.6	Any individual or entity that owns or licenses computerized data that includes personal information must provide notification if unencrypted or unredacted Personal	<p>Notice must be given without unreasonable delay.</p> <p>Notice may be reasonably delayed to allow the individual or entity</p>	<p>Disclosure to be given in one of the following forms:</p> <p>(1) writing (2) electronic notice (3) telephone (4) substitute service</p>	An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or	An entity that maintains its own notification procedures as part of an information policy for the treatment of personal	There is no notice obligation if the entity or individual concludes that there was no reasonable belief that the breach	The Attorney General may bring an action to enforce this section. A civil penalty of not to exceed \$150,000 per breach or a	An entity subject to GLB that maintains procedures for notification of a breach in accordance with the provisions of the Act and any rules,

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>Information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes or is reasonably believed to cause identity theft or another fraud to a resident of Virginia. Disclosure is also required if encrypted personal information is accessed and acquired in unencrypted form or if the security breach involves a person with access to the encryption key and this access has or it is reasonably believed that the breach will cause identity theft or fraud.</p> <p>Notification must also be provided to the Office of the Attorney General.</p> <p>If an individual or entity</p>	<p>to determine the scope of the breach of the security system and restore the reasonable integrity of the system.</p> <p>Notice may be reasonably delayed if a law enforcement agency determines and advises the entity or person that the notice will impede a criminal or civil investigation, or homeland or national security.</p>	<p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$50,000; (ii) the effected class exceeds 100,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); OR (c) notification to major statewide media.</p>	<p>license must notify the owner of licensee of the breach without unreasonable delay following discovery of the breach.</p>	<p>information that is consistent with the timing requirements of the law shall be deemed to be in compliance with this law if it provides notifications in accordance with its procedures.</p>	<p>has caused or will cause, identity theft or another fraud.</p>	<p>series of breaches are discovered in a single investigation.</p> <p>An individual may also bring an action to recover direct economic damages resulting from a violation of this law.</p>	<p>regulations, or guidelines promulgated there is deemed to be in compliance.</p> <p>An entity that complies with the notification requirements or procedures pursuant to the rules, regulations, procedures, or guidelines established by the entity's primary or functional state or federal regulator shall be in compliance with this law.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>provides notice to 1,000 persons at one time under this law the individual or entity must notify, without unreasonable delay, the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notice.</p> <p>Notice to Other Entities Is Required.</p>							
Washington Wash. Rev. Code § 19.225.010	<p>Any person that conducts business in Washington that owns or licenses computerized data that includes Personal Information about a Washington resident must give notice to the affected resident if it becomes aware that Personal Information</p>	<p>Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to</p>	<p>Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if consistent with federal law); or 3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing</p>	<p>Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of any breach immediately</p>	<p>Existing security policies that include notice in the event of a security breach can be followed if they are otherwise consistent with this law and compliance with any federal law requiring notice is</p>	<p>No disclosure is required of a technical breach that does not seem reasonably likely to subject customers to a risk of criminal activity.</p>	<p>Any customer injured by a violation of this statute may institute civil actions to recover damages.</p> <p>Any business that violates this statute may be enjoined.</p>	

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>was, or is reasonably believed to have been, acquired by an unauthorized person.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or state identification card number; or (3) account number or credit/debit card number with any required security code, access code or password.</p>	<p>determine the scope of the breach and restore the reasonable integrity of the system.</p> <p>Notice can be delayed if instructed by law enforcement agencies.</p>	<p>notice would exceed \$250,000; (ii) the effected class exceeds 500,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p>	<p>following discovery of such breach if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person.</p>	<p>in compliance with this statute.</p>		<p>Waivers of this statute are unenforceable.</p>	
<p>Washington D.C.</p> <p>D.C. Code § 28-3851 to -3853</p>	<p>A person or entity that conducts business in Washington D.C. who owns or licenses computerized data that includes Personal Information who</p>	<p>Notification must be made in the most expedient time possible consistent with the needs of law enforcement and the need to</p>	<p>Disclosure to be given in the following forms:</p> <p>1) Written notice; or 2) Electronic notice (if the customer has consented to receipt of</p>	<p>Any person or entity who maintains computerized data that includes personal information that the person does not own</p>	<p>A person or business that maintains its own notification procedures as part of an information security policy for</p>		<p>A resident injured by a violation of this law may bring a civil action to recover actual damages, the costs of the</p>	<p>A person or entity that maintains procedures for a breach notification system under GLB and provides notice in accordance with</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>discovers a breach of a security system must notify any District of Columbia whose personal information was included in the breach.</p> <p>Personal information means an individuals first name or first initial and last name, or phone number, or address and any combination of the following: (1) SSN; (2) Drivers license number or customer identification number; (3) credit/debit card number; (4) any other number or code or combination of numbers or codes that allows access to or use of an individual's financial or credit account.</p> <p>If more than 1,000 persons must be notified of a breach</p>	<p>determine the scope of the breach and restore the reasonable integrity of the data system.</p> <p>Notification may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation.</p>	<p>electronic notice consistent with provisions regarding electronic records under Federal law); or 3) Substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$50,000; (ii) the affected class exceeds 100,000 persons; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide and if appropriate national media.</p>	<p>shall notify the owner or licensee of the information of any breach.</p>	<p>the treatment of personal information and is otherwise consistent with the timing requirements of this law is deemed to be in compliance with the notification requirements of this law if the person or business provides notice in compliance with its policy reasonably calculated to give actual notice. The notice may be given by electronic mail if that is the primary means of communication with the resident.</p>		<p>action, and reasonable attorneys fees. Dignitary damages including pain and suffering may not be recovered.</p> <p>The Attorney General may petition the Superior Court of the District of Columbia for temporary or permanent injunctive relief and an award of restitution resulting from a violation of the law. The Attorney General may recover a civil penalty not to exceed \$100 for each violation, the costs of the action, and</p>	<p>GLB rules, regulations, guidance and guidelines is deemed to be in compliance with the law.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	notification must also be given to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, of the timing, distribution and content of the notices. Notice to other entities required.						reasonable attorney fees. A waiver of this provision is null and void.	
West Virginia W. Va. Code §§ 46A-2A-101 to -105	An individual or entity that owns or licenses computerized data that includes unencrypted or unredacted personal information must give notice of a breach of the security of the system following discovery or notification of the breach to any resident of West Virginia whose information was or is reasonably believed to have been accessed and acquired by unauthorized individual	Notice must be made without unreasonable delay unless steps are necessary to determine the scope of the breach and to restore the reasonable integrity of the system. Notice may be delayed if a law enforcement agency determines and advises the individual or entity that the notice will	Disclosure to be given in the following forms: 1) Written notice; or 2) Electronic notice (if the notice is provided consistent with Federal law); 3) telephonic notice; or 3) Substitute notice. Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$50,000; (ii) the effected class exceeds 100,000 persons; or	An individual or entity that maintains computerized data that includes personalized data that the individual or entity does not own must give notice to the owner or licensee of the information of any breach of security as soon as practicable after the discovery if the personal information was or is reasonably	An entity that maintains it owns notification procedures as part of an information privacy or security policy for the treatment of personal information and that are consistent with the timing requirements of the law is deemed to be in compliance with the law if it notifies residents in accordance with its		Failure to comply with the notice provisions of this law is a violation of West Virginia's unfair and deceptive business practice law. The attorney general has exclusive authority to enforce the law and a civil penalty cannot be assessed unless the court finds that the	A financial institution that provides notification in accordance with the notification guidelines prescribed by the Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice is deemed to be in compliance with this law.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	or the entity reasonably believes has caused or will cause identity theft or other fraud.	impede a criminal or civil investigation or homeland or national security.	<p>(iii) insufficient contact information.</p> <p>Substitute notice must consist of any two of the following: (a) email notice (if email addresses are known); (b) conspicuous posting on website (if one is maintained); and (c) notification to major statewide media.</p> <p>Notice must include to the extent possible: (1) a description of the categories of information that were reasonably believed to have accessed or acquired by an unauthorized person; (2) a telephone number or website address that the individual may use to contact the entity or their agent regarding the breach; (3) a toll-free telephone number</p>	believed to have been accessed and authorized by an unauthorized person.	procedures in the event of a security breach.		defendant has engaged in a course of repeated and willful violations. A civil penalty may not exceed \$150,000 per breach or series of related breaches.	An entity that complies with the notification requirements or procedures pursuant to the rules, procedure, or guidelines established by the entity's primary or functional regulator is deemed to be in compliance with this law.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
			and addresses for major credit organizations and information on how to place a fraud alert or security freeze. Notice content required.					
Wisconsin Wis. Stat. § 134.98	If an entity has a principal place of business in Wisconsin, the entity maintains or licenses Personal Information in Wisconsin or the information pertains to a Wisconsin resident, and it knows there has been an unauthorized acquisition of Personal Information, the entity must take reasonable steps to notify each consumer. Personal Information means an individual's first name or first initial and last name in	Must be given within a reasonable time, but not to exceed 45 days, after learning of acquisition. Notice may be delayed at request of law enforcement agencies, in which case, the 45 days begins to run following authorization of law enforcement to provide notice.	By mail or via a method that the entity has previously used to communicate with the consumer. If a mailing address cannot reasonably be found, and there have been no prior communications, then the entity may use a method reasonably calculated to provide actual notice to the consumer.	If an entity stores data regarding a Wisconsin resident, but does not own or license it, then the person must give notice as soon as practicable to the owner of the data if the person knows there was an unauthorized acquisition.		No notice is required if the acquisition does not create a material risk of identity theft of fraud or the Personal Information was acquired in good faith by an employee or agent if used for a lawful purpose.		Certain entities, including financial institutions regulated by GLB or certain other regulators are exempt.

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or state identification card number; (3) account number or credit/debit card number with any required security code, access code or password; (4) the individual's deoxyribunocleic acid profile; or (5) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.</p> <p>PI definition includes biometric data and genetic data.</p> <p>May include non-computerized data.</p>	<p>Notice in 45 days.</p>						

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
(UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
Wyoming Wyo. Stat. Ann. §§ 40-12-501 to -502	<p>Any commercial entity that conducts business in Wyoming that owns or licenses computerized data that includes Personal Information about a Wyoming resident must give notice of a breach to the affected resident if, after conducting an investigation, determines the misuse of Personal Information of a Wyoming resident has occurred or is reasonably likely to occur.</p> <p>A Breach means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes</p>	<p>Notification of breach must be provided in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. Notice can be delayed if instructed by law enforcement agencies.</p>	<p>Disclosure to be given in one of the following forms: 1) written notice; 2) electronic notice (if consistent with federal law); or 3) substitute notice.</p> <p>Substitute notice is permissible only if: (i) the cost of providing notice would exceed \$10,000 for Wyoming businesses, and \$250,000 for all other businesses; (ii) the effected class exceeds 10,000 Wyoming based persons and 500,000 persons for all other entities; or (iii) insufficient contact information.</p> <p>Substitute notice must consist of: (a) email notice (if email addresses are known); (b) conspicuous posting</p>	<p>Persons that maintain computerized data owned by others that includes Personal Information must give notice to the owner or licensee of the information of any breach immediately following discovery of such breach if the Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person. The person who maintains that date and the owner of the information may agree which person will provide any required notice.</p>			<p>The attorney general may bring an action in law or equity to address any violation of the law and for other relief that may be appropriate.</p>	<p>Financial institutions who comply with requirements of applicable federal laws (15 U.S.C.A. § 6809 or 12 U.S.C.A. § 1752) are deemed to be in compliance with this statute.</p>

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.

INTERNATIONAL SECURITY BREACH NOTIFICATION SURVEY
 (UNITED STATES CONTENT AS OF AUGUST 26, 2009)

State	Notice Requirements	Timing of Disclosure	Form of Disclosure	Entities that Maintain Data	Existing Policies	Exemptions from Disclosure	Damages/ Enforcement	Preemption
	<p>or is reasonably believed to cause loss or injury to a resident of Wyoming.</p> <p>Personal Information means an individual's first name or first initial and last name in combination with any of the following when the data element is not encrypted: (1) SSN; (2) driver's license number or state identification card number; (3) account number or credit/debit card number with any required security code, access code or password; (4) tribal identification card; or (5) federal or state government issued identification card.</p> <p>PI definition includes tribal, federal or state identification cards.</p>		<p>on website (if one is maintained); and (c) notification to major statewide media (must include a toll-free phone number where an individual can learn whether or not the individual's personal data is include in the security breach).</p> <p>Notices to individuals must include a toll-free number that the individual may use to contact the person collecting the data, or his agent, and from which the individual may learn the toll-free contact numbers and addresses for the major credit reporting agencies.</p> <p>Notice content required.</p>					

This document does not replace review of the applicable laws and the US content is based upon Chapter 22 of Andrew Serwin, *Information Security and Privacy: A Guide to Federal and State and Compliance*, (3rd ed. West 2009). It does not constitute legal advice.