

Revised as of December 1, 2008

**SECURITY BREACH RESPONSE GUIDE**

This Guide provides a step-by-step outline of how to respond to a security breach. See below for notice triggers in the various states. A sample consumer notice letter is at Exhibit A. A sample consumer notice letter for Massachusetts residents is at Exhibit B. Contact information for agencies that likewise require notice is at Exhibit C.

<p><b><i>Pre-Breach Planning</i></b></p>	<ul style="list-style-type: none"> <li>• Security breaches may occur due to outside hackers, inside rogue employees, economic espionage, physical intrusion, inadvertence, and third party negligence in managing your data.             <ul style="list-style-type: none"> <li>○ Look at the lifecycle of collection, use, storage, disclosure, and destruction of personal information in your company to understand vulnerabilities.</li> <li>○ Ensure contractual protections are in place with all third party vendors that have access to or possession of customer personal information.</li> <li>○ Ensure your employee access agreements and policies are comprehensive and define the scope of authorized access to your systems.</li> </ul> </li> <li>• Organize Breach Response Team and prepare Incident Response Plan (IRP) now. Choose IRP lead, identify all key personnel, and establish an appropriate communications chain (<i>e.g.</i>, when must the CEO be told?).</li> <li>• Ensure IRP identifies key personnel needed to respond to each item below (<i>e.g.</i>, legal, privacy, risk management, security, public relations).</li> <li>• Conduct a training meeting and scenario planning.</li> <li>• Establish liaison for law enforcement so you know whom to call.</li> </ul>
<p><b><i>Initial Breach Response</i></b></p>	<ul style="list-style-type: none"> <li>• Take immediate steps to correct the security failure and ensure that the breach is contained.</li> <li>• Initiate Incident Response Plan.</li> <li>• Commence evidence gathering and preservation. Ensure forensic procedures are followed. Contact legal immediately. Consider outside consultant if necessary to preserve evidence properly.</li> <li>• Document response efforts and costs of remediation for insurance purposes or to prove damages. Remember, damage amount will be important to establish violation of Computer Fraud and Abuse Act, which has a \$5000 minimum threshold. Further, if a third party is convicted, you will be entitled to restitution under federal and most state sentencing laws and will get a judgment good for ten years against the perpetrator (think about attaching the book royalties when the hacker cashes in on how he or she cracked your system).</li> </ul>

<p><b><i>Threshold Decision: Whether to Notify Law Enforcement</i></b></p>	<ul style="list-style-type: none"> <li>• If the breach is ongoing, or consists of hacking, viruses or other malicious or illegal activity, consider notifying law enforcement immediately.</li> <li>• Contact local U.S. Attorney who can assist in coordination with law enforcement. Alternatively, contact local FBI branch office or Secret Service directly.</li> <li>• IT can invite law enforcement on premises during an attack to assist in the monitoring of communications. <i>See</i> 18 U.S.C. 2511 for computer trespass requirements.</li> <li>• Recommendation: Notify local authorities. Note: Customers may need police report to obtain credit protection or deal with ID theft.</li> </ul>
<p><b><i>Determine Whether Notice is Required or Desirable</i></b></p>	<ul style="list-style-type: none"> <li>• <i>See</i> Perkins Coie's Security Breach Notification Chart at: <a href="http://www.perkinscoie.com/files/upload/securitybreach.pdf">http://www.perkinscoie.com/files/upload/securitybreach.pdf</a></li> <li>• Notice usually triggered by a computer breach resulting in disclosure of personal information, usually defined as Name + (1) SSN, (2) driver's license #, or (3) financial account number plus PIN or password. Check for state differences.</li> <li>• For telecommunications carriers, note the requirement to provide notice for a breach of security resulting in the loss of customer proprietary network information or CPNI. 47 C.F.R. § 2011.</li> <li>• Decide whether to notify consumers for <i>any</i> loss of PI even if statutory trigger is not present.</li> <li>• Decide whether to notify all customers, not just those in states requiring notice. Some AGs believe it is an unfair practice not to notify residents even though the state does not have notice requirements.</li> <li>• There are no requirements today for notification of foreign resident customers although the EU, Canada and New Zealand currently are considering such guidance or requirements.</li> </ul>
<p><b><i>Pre-Notice Planning and Preparation</i></b></p>	<ul style="list-style-type: none"> <li>• Plan for high volume of customer service calls. Draft script for CSRs; obtain outside call center service if needed. Prepare PR spokesperson to handle questions about the breach from media. Note: you should identify call center support as part of planning; it takes time to negotiate call center contract.</li> <li>• If third party bailee or vendor gives notice of the breach to your customers, ensure customer service is prepared for calls from legitimate customers as well as phishing attempts by bad actors seeking customer information as a result of seeing the letter in the media. Obtain a copy of the notice sent to consumers and contractually require the right to approve content of the notice, when possible.</li> <li>• Consider creating Web site FAQ on security breach, contact info for credit reporting agencies, and link to FTC identity theft advice</li> </ul>

	at <a href="http://www.consumer.gov/idtheft">www.consumer.gov/idtheft</a> .
<b><i>Notify State Attorney Generals and Agencies as Required</i></b>	<ul style="list-style-type: none"> <li>• For companies giving notice to Maryland residents, give notice to the State AG before notifying Maryland residents.</li> <li>• For companies giving notice to New Jersey residents, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling before giving notice to New Jersey residents.</li> <li>• For companies giving notice to New York residents, notify the state AG, the Consumer Protection Board, and the state Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and approximate number of affected persons before giving notice to New York residents. You can use the security breach reporting form located on page 14 of the document located at: <a href="http://www.consumer.state.ny.us/pdf/the_new_york_business_guide_to_privacy.pdf">http://www.consumer.state.ny.us/pdf/the_new_york_business_guide_to_privacy.pdf</a></li> </ul>
<b><i>Notify Credit Bureaus in Advance of Notice to Customers</i></b>	<ul style="list-style-type: none"> <li>• Credit bureaus will have to be prepared to respond to incoming calls requesting credit freeze or fraud protection. Contact the credit bureaus before notifying customers.</li> </ul>
<b><i>Notify Customers</i></b>	<ul style="list-style-type: none"> <li>• Determine whether to notify consumers individually or use substitute notification procedures (if available). We do not recommend using substitute notification procedures except where individual notification would be cost-prohibitive or unavailable.</li> <li>• For individual notices, determine whether email, phone, written or fax notices are most appropriate. Make sure that notice method is allowed in the state in which you use it and be aware of other restrictions (e.g., email notice typically requires E-SIGN compliance).</li> <li>• Most statutes do not specify the notice's content, but a few have minimum requirements. For financial institutions, <i>see</i> Interagency Guidance on Response Programs for Security Breaches which contains notice requirements. Make sure the envelope is designed to increase the likelihood of actual review (some state AG's have complained that notices look too much like spam).</li> <li>• 90-Day Fraud Alerts: Customers can contact credit bureau to add a fraud alert message to their credit reports free of charge so credit providers will require positive ID before extending credit.</li> <li>• 7-Year Freezes: Customers can request Extended Fraud Victim Alert by submitting a copy of a valid ID theft report filed with any law enforcement agency. An Alert will remain on the report for 7 years and may cause customer delay in obtaining credit.</li> </ul>
<b><i>Other Notices</i></b>	<ul style="list-style-type: none"> <li>• If the breach involves credit card information, comply with your merchant agreement, PCI standards and other pertinent rules.</li> </ul>

	<p>Notify your merchant bank and your card issuer. If Visa cardholders are affected, also contact Visa's Fraud Control Group at (650) 432-2978.</p> <ul style="list-style-type: none"> <li>• Notify the Secret Service if financial or credit card payment information was compromised.</li> <li>• Notify state AGs and agencies as required (see list in Exhibit C). If the breach is widespread, consider notifying state AGs even if not required by statute.</li> <li>• Evaluate whether you have any notice obligation to insurers.</li> <li>• If you are holding another company's data, evaluate your contract and statutory obligations to provide notice to data owner.</li> </ul>
<i>Consider Fraud Insurance</i>	<ul style="list-style-type: none"> <li>• Some entities suffering breaches purchase fraud protection insurance from credit reporting agencies for their customers for one year. Consider this insurance as a customer goodwill gesture.</li> </ul>
<i>Customer Rights</i>	<ul style="list-style-type: none"> <li>• See <a href="https://www.experian.com/consumer/cac/01_loginInfo7.htm">https://www.experian.com/consumer/cac/01_loginInfo7.htm</a> for a summary of customer rights for ID theft victims.</li> <li>• Be prepared to assist customers who claim identity theft from the breach and know what information you have to release upon request.</li> </ul>
<i>Remedies</i>	<ul style="list-style-type: none"> <li>• As noted above, a victim of a security breach, the company may have remedies against the perpetrator, if known. If any individual is prosecuted, the company will have the right to restitution under the Victim and Witness Protection Act.</li> <li>• Companies should understand their role in any criminal prosecution or sentencing of a computer hacker or other data thief. Company will want to ensure that its security procedures and intellectual property do not become part of the evidence in the case and subject to further public disclosure.</li> </ul>
<i>Evaluate Litigation Risk</i>	<ul style="list-style-type: none"> <li>• Some states have passed or are considering imposing liability on the merchant whose systems have suffered a security breach for the costs associated with re-issuance of credit cards. Issuing banks have lost cases seeking damages against such merchants due to the absence of privity of contract with the merchant and a lack of a duty of care flowing to the issuing banks. These statutes would create a cause of action for such a loss.</li> <li>• Individuals may sue alone or in a class action for damages related to identity theft on various tort or contract theories. Businesses should evaluate their privacy policies and customer agreements to ensure that they allocate risk appropriately.</li> <li>• Federal and state agencies may inquire into the circumstances of a security breach involving consumer personal information.</li> <li>• For companies with Safe Harbor coverage for data derived from EU residents, be alert to FTC oversight of such breaches and expect inquiry regarding same.</li> </ul>

**EXHIBIT A - FORM OF CONSUMER NOTIFICATION FOR ALL STATES BUT  
MASSACHUSETTS**

*[Company Letterhead] [If letterhead is not used, provide contact information.]*

TO: *[The notice need not be personalized, you only need to demonstrate that it went to each individual]*

You are receiving this notice because \_\_\_\_\_. *[Describe breach in general terms, e.g., "a computer was stolen containing certain personal information," including the approximate date of the breach, and briefly specify what information was compromised, e.g. SSNs, driver's license numbers, credit card numbers. If SSNs, credit card numbers, passwords or other types of easily-recognizable or particularly sensitive PI were not stolen, note it here.]* We do not have any evidence that this data has been *[accessed, used or disclosed]*. *[Make sure this is true.]* We are providing you this notice to alert you to the possibility of attempted identity theft and to explain the steps we have taken to protect against identity theft or abuse of the information.

*[Describe what has been done to protect the information from further unauthorized access]* We *[have contacted] [are in the process of contacting]* the three nationwide credit reporting agencies to place a fraud alert on your credit report. An initial fraud alert remains on your report for a period of 90 days. You will receive a free credit report from each of the three companies and you should review the reports and your account statements carefully to identify any problems.

A fraud alert on your credit report does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information may have been compromised and requires them to verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. While this may cause some short delay if you are the one applying for the credit, it ensures against someone else obtaining credit in your name.

For your information, here is the contact information for the credit reporting agencies in case you have questions about the fraud alert or how to read your free credit report; you may also contact the credit reporting agencies to extend a fraud alert for a longer period of time or reinstitute a fraud alert at a later date:

**Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241

**Experian:** 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013

**TransUnion:** 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

*[We want you to know that we are cooperating fully with the investigation of this incident by law enforcement.] [Delete if inapplicable.]* Again, we have no information to suggest that the *[information on the stolen computer] [information on the compromised network] [compromised information]* has been *[misused for purposes of identity theft] [This should be the same as above.]*, but we want to ensure that you are forewarned and able to identify any suspicious account activity. In addition, the Federal Trade Commission maintains a helpful Web site at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) to help guard against identity theft.

Finally, \_\_\_\_\_. *[Describe measures, if any, that you have taken to allow customers to get more information (e.g., a telephone assistance line, a Web site with information, etc.)]* If you suspect that you are a victim of identity theft, you should immediately contact the police. Provide them a copy of this notice so that we can assist them with any investigation.

We are committed to protecting your privacy and we apologize for any concern this may cause you.

*[Insert signature block.]*

*[Addendums for specific states. If you must notify residents in one of the below states, include the language for that state in the notification letter.]*

**For residents of Vermont:**

We have set up a toll-free telephone line that you may call for further information and assistance.

**For residents of Maryland:**

You can obtain information from these sources about steps you can take to avoid identity theft:

Maryland Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
www.oag.state.md.us

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
1-877-IDTHEFT (438-4338)  
www.ftc.gov/bcp/edu/microsites/idtheft/

**For residents of West Virginia:**

You may contact us at \_\_\_\_\_ *[telephone number]* or \_\_\_\_\_ *[website address]* to learn what types of personal information we maintain and whether or not we maintained information about you.

To further protect yourself, you may request a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit. To place a security freeze on your credit report, send a request by mail to a consumer reporting agency at the address below that includes the following (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past two years; and (5) any applicable incident report or complaint with a law enforcement agency or the Division of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.30 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

**Equifax Security Freeze**, P.O. Box 105788, Atlanta, Georgia 30348

**Experian Security Freeze**, P.O. Box 9554, Allen, TX 75013

**TransUnion Fraud Victim Assistance Division**, P.O. Box 6790, Fullerton, CA 92834-6790

**For residents of Wyoming:**

We have set up a toll-free number that you may call for further information and assistance, including the toll-free contact telephone numbers and addresses for the major credit reporting agencies cited above.

## EXHIBIT B - FORM OF CONSUMER NOTIFICATION FOR MASSACHUSETTS

*[Company Letterhead] [If letterhead is not used, provide contact information.]*

TO: *[The notice need not be personalized, you only need to demonstrate that it went to each individual]*

You are receiving this notice because a security breach may have exposed your personal information.\_\_\_\_\_. *[Briefly specify what information was compromised, e.g. SSNs, driver's license numbers, credit card numbers. If SSNs, credit card numbers, passwords or other types of easily-recognizable or particularly sensitive PI were not stolen, note it here.]* We do not have any evidence that this data has been *[accessed, used or disclosed]*. *[Make sure this is true.]* We are providing you this notice to alert you to the possibility of attempted identity theft and to explain the steps we have taken to protect against identity theft or abuse of the information.

*[Describe what has been done to protect the information from further unauthorized access] We [have contacted] [are in the process of contacting] the three nationwide credit reporting agencies to place a fraud alert on your credit report. An initial fraud alert remains on your report for a period of 90 days. You will receive a free credit report from each of the three companies and you should review the reports and your account statements carefully to identify any problems.*

A fraud alert on your credit report does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information may have been compromised and requires them to verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. While this may cause some short delay if you are the one applying for the credit, it ensures against someone else obtaining credit in your name.

For your information, here is the contact information for the credit reporting agencies in case you have questions about the fraud alert or how to read your free credit report; you may also contact the credit reporting agencies to extend a fraud alert for a longer period of time or reinstitute a fraud alert at a later date:

**Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241

**Experian:** 1-888-EXPERIAN (397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013

**TransUnion:** 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

To further protect yourself, you may request a security freeze on your credit report. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent; however, using a security freeze may delay your ability to obtain credit. To place a security freeze on your credit report, send a request by mail to a consumer reporting agency at the address below that includes the following (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past two years; and (5) any applicable incident report or complaint with a law enforcement agency or the

Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

**Equifax Security Freeze**, P.O. Box 105788, Atlanta, Georgia 30348

**Experian Security Freeze**, P.O. Box 9554, Allen, TX 75013

**TransUnion Fraud Victim Assistance Division**, P.O. Box 6790, Fullerton, CA 92834-6790

You have the right to obtain a police report regarding the security breach. *[We want you to know that we are cooperating fully with the investigation of this incident by law enforcement.] [Delete if inapplicable.]* Again, we have no information to suggest that the compromised information has been *[misused for purposes of identity theft] [This should be the same as above.]*, but we want to ensure that you are forewarned and able to identify any suspicious account activity. In addition, the Federal Trade Commission maintains a helpful Web site at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) to help guard against identity theft.

Finally, \_\_\_\_\_. *[Describe measures, if any, that you have taken to allow customers to get more information (e.g., a telephone assistance line, a Web site with information, etc.)]* If you suspect that you are a victim of identity theft, you should immediately contact the police. Provide them a copy of this notice so that we can assist them with any investigation.

We are committed to protecting your privacy and we apologize for any concern this may cause you.

*[Insert signature block.]*

## EXHIBIT C

### CONTACT INFORMATION

#### I. CREDIT REPORTING AGENCIES

##### A. Contact Information for Reporting Breaches

Equifax	Experian	TransUnion
U.S. Consumer Services Equifax Information Services, LLC Phone: (678) 795-7971 businessrecordsecurity@equifax.com	Experian Data Breach Support Phone: 1-866-751-1323 businessrecordsvictimassistance@experian.com	TransUnion Data Breach Reporting Hotline: Phone: 1-800-971-4307 http://www.transunion.com

##### B. Fraud Alert Contact Information to Include in Notices to Consumers

Equifax	Experian	TransUnion
Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 Phone: (888) 766-0008	Experian National Consumer Assistance P.O. Box 2104 Allen, TX 75013-2104 Phone: (888) 397-3742	Fraud Victim Assistance Department P.O. Box 6790 Fullerton, CA 92634-6790 Phone: (800) 680-7289 Fax: (714) 447-6034

#### II. STATE AGENCIES

State	Recipients Requiring Notice
Louisiana	<p>When notice to Louisiana citizens is required by the statute, the Entity shall provide written notice detailing the breach of the security of the system to the Consumer Protection Section of the Attorney General's Office. Notice shall include the names of all Louisiana citizens affected by the breach. Failure to provide timely notice may be punishable by a fine not to exceed \$5,000 per violation. Notice to the attorney general shall be timely if received within 10 days of distribution of notice to Louisiana citizens. Each day notice is not received by the attorney general shall be deemed a separate violation.</p> <p>Written notification shall be mailed to: Louisiana Department of Justice Office of the Attorney General Consumer Protection Section 1885 N. Third Street Baton Rouge, LA 70802</p>

Maine	<p>When notice of a breach of the security of the system is required, the Entity shall notify the appropriate state regulators within the Department of Professional and Financial Regulation, or if the person is not regulated by the department, the AG.</p> <p>State of Maine Office of the Attorney General 6 State House Station Augusta, Maine 04333</p>
Maryland	<p>Prior to giving the notification required under the statute, an Entity shall provide notice of a breach of the security of a system to the Maryland Office of the AG. Include a brief description of the nature of the security breach, the number of Maryland residents being notified, what information has been compromised, any steps the business is taking to restore the integrity of the system, and a sample copy of the notice being sent to consumers.</p> <p>Office of the Attorney General Attn: Security Breach Notification 200 St. Paul Place Baltimore, MD 21202 Fax: (410) 576-6566 ldtheft@oag.state.md.us</p>
Massachusetts	<p>Companies notifying Massachusetts residents must also provide notice as soon as practicable and without unreasonable delay to the Massachusetts AG and the Massachusetts Director of Consumer Affairs and Business Regulation. The notice to be provided to the AG and Director of Consumer Affairs shall include, but not be limited to (i) the nature of the breach of security or unauthorized acquisition or use, (ii) the number of residents of MA affected by such incident at the time of notification, and (iii) any steps the Entity has taken or plans to take relating to the incident.</p> <p>Commonwealth of Massachusetts Office of the Attorney General One Ashburton Place Boston, MA 02108</p> <p>Director of Consumer Affairs and Business Regulation 10 Park Plaza, Room 5170 Boston, MA 02116</p>
New Hampshire	<p>Companies engaged in trade or commerce that are subject to RSA 358-A:3, I (trade or commerce that is subject to the jurisdiction of the bank commissioner, the director of securities regulation, the insurance commissioner, the public utilities commission, the financial institutions and insurance regulators of other states, or federal banking or securities regulators who possess the authority to regulate unfair or deceptive trade practices) must notify the regulator which has primary regulatory authority over such trade or commerce.</p> <p>All other Entities must notify the NH AG.</p>

	<p>The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in NH who will be notified.</p> <p>State of New Hampshire Office of the Attorney General 33 Capitol Street Concord, NH 03301</p>
New Jersey	<p>In advance of the disclosure to New Jersey residents, the company must report the breach of security and any information pertaining to the breach to the New Jersey State Police</p> <p>New Jersey State Police P.O. Box 7068 West Trenton, NJ 08628</p>
New York	<p>If any New York residents are to be notified, the Entity must notify the state AG, the Consumer Protection board, and the state Office of Cyber Security and Critical Infrastructure Coordination as to the timing, content and distribution of the notices and approximate number of affected persons. The New York State Security Breach Reporting Form is located on page 14 of the document located at: <a href="http://www.consumer.state.ny.us/pdf/the_new_york_business_guide_to_privacy.pdf">http://www.consumer.state.ny.us/pdf/the_new_york_business_guide_to_privacy.pdf</a></p> <p><b>SECURITY BREACH NOTIFICATION</b> New York State Office of Cyber Security &amp; Critical Infrastructure Coordination 30 South pearl Street, Floor P2 Albany, NY 12207 Fax: 518 - 474 - 9090 E - mail: <a href="mailto:info@cscic.state.ny.us">info@cscic.state.ny.us</a></p> <p><b>SECURITY BREACH NOTIFICATION</b> New York State Consumer Protection Board 1740 Broadway, 15th floor New York, NY 10019 Fax: 212 - 459 - 8855 E - mail: <a href="mailto:security_breach_notification@consumer.state.ny.us">security_breach_notification@consumer.state.ny.us</a></p> <p><b>SECURITY BREACH NOTIFICATION</b> Consumer Frauds &amp; Protection Bureau New York State Attorney General's Office 120 Broadway – 3rd Floor New York, NY 10271 Fax: 212 - 416 - 6003 E - mail: <a href="mailto:breach.security@oag.state.ny.us">breach.security@oag.state.ny.us</a></p>

North Carolina	<p>For companies notifying more than 1,000 North Carolina residents, notice must be given to the Consumer Protection Division of the North Carolina AG's Office.</p> <p>Consumer Protection Division  North Carolina Attorney General's Office  Department of Justice  9001 Mail Service Center  Raleigh, NC 27699-9001</p>
Puerto Rico	<p>Notice must be given to DACO within 10 days of discovering the breach.</p> <p>Departamento de Asuntos del Consumidor  Apartado 41059  Minillas Station  Santurce, PR  00940</p>
Virginia	<p>For companies notifying Virginia residents, notice must also be given to the Office of the Virginia AG. If more than 1,000 residents are notified, notification of the timing, distribution and content of the notice to residents must also be given.</p> <p>Office of the Attorney General  900 East Main Street  Richmond, VA 23219</p>

### III. FEDERAL AUTHORITIES

FBI	<p>If notifying the FBI, contact your local field office. Contact information: <a href="http://www.fbi.gov/contact/fo/fo.htm">http://www.fbi.gov/contact/fo/fo.htm</a>.</p>
U.S. Secret Service	<p>If the U.S. Secret Service is to be notified, contact the field office closest to your company by using the contact information at <a href="http://www.secretservice.gov/field_offices.shtml">http://www.secretservice.gov/field_offices.shtml</a>. The Secret Service will likely require your company to submit a Cyber Threat / Network Incident Report Form (Secret Service Form 4017).</p>
U.S. Attorneys	<p>Contact information for U.S. Attorneys:  <a href="http://www.usdoj.gov/usao/offices/index.html">http://www.usdoj.gov/usao/offices/index.html</a>.</p>