

**Schafer, Scott (AGO)**

**From:** John Chinkes [jchinkes@nita.org]  
**Sent:** Wednesday, May 28, 2008 3:31 PM  
**To:** Schafer, Scott (AGO)  
**Subject:** RE: Data breach at National Institute for Trial Advocacy

The other group indicated I should fill out an on-line form so I asked them what the URL is for that form. We are working on a mail merge to get a printed letter (on letterhead) to all affected customers. I will forward that document to you shortly.  
9 residents (billing address) of MA are affected.

Thanks for the help!

JEMC

**John Chinkes**  
Manager IT  
National Institute for Trial Advocacy  
Direct: 303.953.6838  
E-mail: jchinkes@nita.org



---

**From:** Schafer, Scott (AGO) [mailto:Scott.Schafer@state.ma.us]  
**Sent:** Wednesday, May 28, 2008 1:21 PM  
**To:** John Chinkes  
**Cc:** Schafer, Scott (AGO)  
**Subject:** RE: Data breach at National Institute for Trial Advocacy

Mr. Chinkes:

You may provide written notice to our office via email; however, your notice should include the three data elements required pursuant to G.L. ch. 93H and as set forth in my response to your email. Your initial email did not identify the number of Massachusetts residents affected by the data breach as required by the statute and therefore did not constitute proper notice. I hereby request that you provide that information. In addition, you should include a copy of the sample notice you are sending to consumers as I noted in my response. You may either send that as an attachment to an email or under a separate cover. Please note that you should contact the Office of Consumer Affairs and Business Regulation separately to determine if they will accept email notification.

In terms of notice to consumers, the statute sets forth the proper manner in which to notify affected Massachusetts residents and I refer you to G.L. ch. 93H so that you may determine whether you may notify by email, regular mail or substitute notice.

Scott Schafer  
Assistant Attorney General

---

**From:** John Chinkes [mailto:jchinkes@nita.org]  
**Sent:** Wednesday, May 28, 2008 3:06 PM  
**To:** Schafer, Scott (AGO)  
**Subject:** RE: Data breach at National Institute for Trial Advocacy

5/28/2008

I am guessing that by in writing you don't mean another email? Is that a generational thing: printing the email is paper after all...

JEMC

**John Chinkes**

Manager IT

National Institute for Trial Advocacy

Direct: 303.953.6838

E-mail: [jchinkes@nita.org](mailto:jchinkes@nita.org)



---

**From:** Schafer, Scott (AGO) [<mailto:Scott.Schafer@state.ma.us>]  
**Sent:** Wednesday, May 28, 2008 8:11 AM  
**To:** John Chinkes; Steve Gibson  
**Cc:** Schafer, Scott (AGO)  
**Subject:** RE: Data breach at National Institute for Trial Advocacy

Dear Mr. Chinkes:

I am in receipt of your email correspondence of May 27, 2008 informing this office of a data breach involving the NITA website. Pursuant to G.L. ch. 93H, if you know or have reason to know that the personal information of a Massachusetts resident was acquired or used by an unauthorized person or the subject of a breach of security, you must provide notice in writing, as soon as practicable and without unreasonable delay, to the Attorney General and the Director of Consumer Affairs and Business Regulation. This notice shall include: 1) the nature of the breach of security or unauthorized acquisition or use; 2) the number of Massachusetts residents affected; and 3) the steps you are taking, or plan to take, relating to the incident.

Pursuant to G.L. ch. 93H, you shall also provide notice to affected Massachusetts residents whose personal information was compromised. This notice shall include information concerning: 1) their right to obtain a police report; 2) how a consumer may request a security freeze; 3) the necessary information they will need to provide when requesting a security freeze; and 4) any fees required to be paid to any of the consumer reporting agencies. I refer you to G.L. ch. 93 §§ 56 and 62A for more information concerning security freezes and applicable legal requirements. In addition, in order to ensure compliance with G.L. ch. 93H, we also request that you provide us with a sample of the notice you provide to affected Massachusetts resident and a description of how the notice was provided.

If you should have any questions, please do not hesitate to contact me at 617-727-2200 x2516.

Very truly yours,

Scott D. Schafer

5/28/2008

Assistant Attorney General  
Consumer Protection Division  
Office of Massachusetts Attorney General Martha Coakley

**From:** John Chinkes [mailto:jchinkes@nita.org]  
**Sent:** Tuesday, May 27, 2008 5:53 PM  
**To:** Steve Gibson  
**Subject:** Data breach at National Institute for Trial Advocacy

To Whom It May Concern:

It is with sincere regret that I inform you of a data breach of the NITA web site. On May 13th we discovered that orders placed with us have been viewed by persons unknown outside of our company. It is our belief that credit card information for people in your state has been compromised.

We have taken every step in correcting the errors that led to your information exposure. While we have always used 128 SSL encryption of transactions via our web site, a coding error on a single page allowed illicit access to our web site database. We have fixed this error on that page, examined all other pages for that error, and made significant changes to our payment processing procedures to ensure that this will not happen again.

If you have any questions about this data breach, please contact me or Steve Gibson, COO

Sincerely,

JEMC

**John Edward Max Chinkes**  
Manager IT  
National Institute for Trial Advocacy  
361 Centennial Pkwy., Ste. 220  
Louisville, CO 80027-1284  
Direct: 303.953.6838  
Toll Free: 877.648.2632  
Fax: 720.890.7069  
E-mail: jchinkes@nita.org

  
*Teaching the Art of Advocacy*

5/28/2008

«fullname»  
«address1\_line1»  
«address1\_line2»  
«address1\_line3»  
«address1\_city», «address1\_stateorprovince»  
«address1\_postalcode»  
[LAST 4 DIGITS OF CUSTOMER'S CREDIT CARD # IF YOU HAVE IT]

Dear «salutation» «lastname»:

We are writing to you because of a recent security incident relating to personal information regarding certain customers of the National Institute of Trial Advocacy ("NITA") who placed orders through our website at [www.nita.org](http://www.nita.org). Between February 20, 2008 and May 13, 2008, unauthorized individuals obtained remote access to one of our servers and viewed the customer information for purchases made through our website during that period of time. This information included customer names, addresses, telephone numbers, e-mail addresses, credit card numbers with expiration dates, and, if provided, state bar number and demographic information. We believe that your information was among the information that was viewed.

If we have a credit card number on file for you, the four numbers following your name and address above are the last four numbers on that credit card. If you do not see four numbers following your name and address above, we do not currently have a credit card number on file for you, but your name, address, and other personal information may still have been viewed in this security breach.

**What are the risks of this information being used?**

We do not know what these individuals intend to do with the customer information, and we do not have any evidence that this information has been used in any manner. However, we have no reason not to think these individuals will use the customer information for fraudulent purposes.

**What are we doing to protect your interests?**

We have notified and are working closely with law enforcement authorities to attempt to discover the identity of the thieves;  
We are notifying the NITA customers we believe may have been affected, so that they can take appropriate steps to protect themselves against credit card fraud;  
We have notified the three major credit bureaus of this security breach;  
We have notified Visa, MasterCard, American Express and Discover Card of this security breach;  
We have contacted the merchant bank through which the credit card transactions were processed;  
We have established a toll-free telephone number and e-mail address for our customers to contact with questions regarding this security breach; and  
We have implemented security procedures to prevent future security breach incidents.

### What steps can I take to protect myself?

To protect yourself from the possibility of credit card fraud, we recommend that you immediately contact the company that issued the credit card you used to make purchases from NITA. Tell them that your account may have been compromised and that you wish to close it. If you want to open a new account with the same company, ask them to give you a PIN or password. This will help control access to the account.

You may also want to place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus and tell them that your personal information was accessed in a security breach incident. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax  
800-525-6285

TransUnionCorp  
800-680-7289

Experian  
888-397-3742

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call the credit reporting agency at the telephone number on the credit report. Then contact your local police or sheriff's office and file a police report. Get a copy of the police report; many creditors want the information it contains to absolve you of the fraudulent debts.

Even if you do not find suspicious activity on your initial credit reports, experts recommend that you monitor your account statements carefully and obtain and review your credit reports every three months for at least a year. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

**Maryland and Massachusetts residents** have the right to place a security freeze on their consumer reports. A security freeze is designed 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. You may request that a freeze be placed on your consumer report by sending a request to one of the three major credit bureaus by certified mail, overnight mail or regular stamped mail to the address below (check the credit bureau's website for additional information, as some may allow submission of documents by fax as well).

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
www.equifax.com

TransUnion (FVAD)  
P.O. Box 6790  
Fullerton, CA 92834-6790  
www.transunion.com

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
www.experian.com

The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's consumer report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past two years; and applicable fee (if any, as stated on the credit bureau's website) or incident report or complaint with a law enforcement agency. The request also should include a copy of a government issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement, or other information as stated on the credit bureau's website. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The consumer reporting agency may charge a reasonable 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 have submitted a valid police report relating to the identity theft to the consumer reporting agency. Massachusetts residents have the right to obtain a police report if they are the victim of identity theft.

You may obtain information about avoiding identity theft from the FTC at:

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/](http://www.ftc.gov/bcp/edu/microsites/idtheft/)

You also should file a complaint with the FTC (at the same contact information above). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

In addition, **Maryland residents** may obtain information from the Maryland Attorney General's Office.

Office of the Attorney General Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

**How can I get more information?**

If you have any questions or concerns and you wish to contact our office, you may call us at \_\_\_\_\_, e-mail us at [DataSecurity@NITA.org](mailto:DataSecurity@NITA.org) or write us at 361 Centennial Pkwy STE 220 Louisville, CO 80027

We deeply regret this incident and apologize to you and all of our customers for the inconvenience it may cause you.

Sincerely,

Steve Gibson

COO