Facsimile Transmittal

FAX

To: 'New_Hampshire_Attorney_General' From: John R. Christiansen
Company: Date: 03/20/2012
Fax Number: 16032712110 Pages: 6 (including cover page)
Re: Notification of Security Breach

Comments:

John R. Christiansen
Christiansen IT Law
Phone: 206.301.9412

Please note that email is not necessarily protected against interception by unauthorized individuals, and that email addresses can be falsified, so that there is no guarantee that this email is from the address of the sender. Please contact me by phone if you would prefer to use a secure messaging service. If you are concerned that the message may be spoofed, please contact directory assistance for my phone number.

March 20, 2012

Michael A. Delaney
Office of the Attorney General
State of New Hampshire
Department of Justice
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of Security Breach

Dear Attorney General Delaney:

I represent Sailboat Owners, Inc., a Washington corporation headquartered in Seattle, Washington ("Company"). I am writing to notify you on behalf of the Company of a breach of security involving two New Hampshire residents.

NATURE OF THE SECURITY BREACH

The Company is a small business which has for several years maintained a retail sales website at http://shop.sailboatowners.com/.

On the morning of 23 February 2012 Company staff noticed unusual activity on the Company's web servers which led them to suspect the network was under attack by intruders. The Company immediately shut down the access and retained Coalfire Associates, http://www.coalfire.com/Home, to assist in preventing further compromise and conduct a forensic investigation.

This investigation indicated that an attack routed from Hanoi, Vietnam uploaded malware to the e-commerce web server at 10:04 am on 22 February 2012, and that database tables containing unencrypted cardholder data were accessed at 4:36 pm on 22 February 2012. Remediation and investigation began on 23 February at 10:40 am. The intrusion did not affect a much larger database in which encrypted records are stored.

Christiansen IT Law
2212 Queen Anne Avenue N.
#333
Seattle, WA 98109

Office:
206.301.9412
Cell: 206.683.9125
Fax: 206.219.6684

Email:
john@christiansenlaw.net
Web: www.christiansenlaw.net

The total number of unencrypted credit cards on the server was initially estimated at 2,485. Subsequent analysis indicated that 2,258 credit card records had been affected. The information in the records included name, credit card number, CVV code and expiration date. The credit cards were issued by Visa, MasterCard and American Express. The records were from 21 transactions which occurred in 2007; 20 which occurred in 2008; 145 which occurred in 2009; 153 which occurred in 2010; 700 which occurred in 2011; and 207 which occurred in 2012.

Forensic investigation allowing specification of affected records was concluded on Tuesday 14 March 2012. The records were then reconciled with other Company records to allow identification of addresses and probable residency of affected individuals by Friday 16 March 2012. Notifications were sent by first class mail to all affected individuals on Monday 19 March 2012.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Two individuals whose Company records indicate that they have New Hampshire addresses, and are therefore presumed to be New Hampshire residents, had personal information which was the subject of this incident. These individuals will shortly receive notice pursuant to New Hampshire law by first class mail. A copy of this notification accompanies this letter.

STEPS YOU HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

Due to the international source of the breach this incident was reported to the U.S. Federal Bureau of Investigation. It has also been reported to the Company's merchant bank, Bank of America; to Visa, MasterCard and American Express; and to Equifax, Experian and Trans Union.

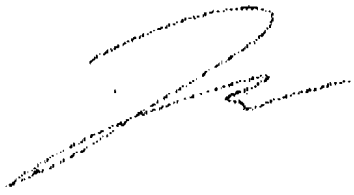
In addition to the remediation and investigative steps indicated above the Company has already initiated a transition to a new ecommerce system which will not entail storage of credit card numbers. An assessment of the Company's systems against Payment Card Industry (PCI) standards and requirements is being scheduled with mitigation of any noncompliance anticipated.

OTHER NOTIFICATION AND CONTACT INFORMATION

Please contact me at my letterhead address, phone, email or fax if you have any questions or need further information. Thank you for your attention.

Very truly yours,

CHRISTIANSEN IT LAW



John R. Christiansen

Attachments: Breach Notification Form Letter

SailboatOwners.com
2130 Westlake Avenue N #2
Seattle WA 98109

Customer Name
Address Line 1
Address Line 2
City State Zip

March 17, 2012

Dear [customer name] ,

On the monring of February 23, 2012, our staff noticed unusual activity on our web servers which led us to believe our network was under attack by intruders. We acted quickly and by later that morning the activity had been stopped.

A data security firm was immediately hired to perform a forensic investigation to determine if there was a data breach. Their report indicated our systems were compromised by a hacker in Hanoi, Vietnam, who installed malicious software which could have compromised data from a limited number of transactions. Unfortunately, your transaction was among them and your contact information and credit card details could have been stolen from our server.

We have no way of knowing if your personal information was actually stolen and fraudulently used as a result of this breach, but we urge you to review your most recent statements to confirm all transactions have been authorized by you. We also urge you to consider obtaining a credit report from a credit reporting bureau. You can obtain such a report free from the service identified on the back of this letter.

Please report any suspicious activity to your card issuing bank or financial institution using the phone number on the back of your card. Some states require that this notification include contact information for credit reporting bureaus and that information can also be found on the back of this letter.

In addition to notifying you, we also reported the incident to the FBI, Visa, MasterCard, American Express, and Discover. Some states require notification to state agencies of security breaches affecting residents of their state, and have established reporting procedures. We have notified the appropriate agencies in such states.

We have also taken immediate steps to enhance our security to guard against future attacks. We are upgrading parts of our system and have hired third party security experts to audit and test it for vulnerabilities.

Our most significant change was to implement a new checkout system that sends your payment information directly to a payment gateway so it is not stored on our servers. The gateway, Authorize.Net, manages billions of transactions for hundreds of thousands of merchants, and is a wholly owned subsidiary of Visa.

Please know we feel terrible about this situation. It's the first problem we've had in 16 years of online transactions. We take pride in our customer service and the possibility of causing you inconvenience is painful to us.

If you have any questions, please call toll free 877-932-7245 from 9am to 4:30pm Pacific time, Monday through Friday.

Again, we are extremely sorry for any inconvenience this may have caused you, and we will do everything in our power to earn your trust in the future.

Sincerely,

Phil Herring
Vice President

Bly Berken
President

The Federal Trade Commission (www.ftc.gov) recommends that you check your credit reports annually.

Review your most recent credit card statement and bank statements to confirm all transactions have been authorized by you. Please report any suspicious activity to your card issuing bank using the number on the back of your card.

Carefully review your credit report. Free credit reports can be obtained from AnnualCreditReport.com:

www.annualcreditreport.com

Annual Credit Report Request Service

P.O. Box 105281

Atlanta, GA 30348-5281

1-877-322-8228

If you have any concerns, 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. As soon as one credit bureau confirms your fraud alert, the others are notified to do the same.

Equifax	Experian	Trans Union Corp
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com
Equifax Credit Services, Inc	Experian	TransUnion LLC
P.O. Box 740241	475 Anton Blvd.	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information is sometimes held for later use or combined with information from other sources. Checking your credit reports periodically can help you spot problems and address them quickly.

You can send mail to the Federal Trade Commission at: 600 Pennsylvania Avenue, NW
Washington, DC 20580

The FTC website is: www.ftc.gov
The FTC Theft helpline: 1-877-438-4338 TTY: 1-866-653-4261