

Stuart P. Ingis

August 4, 2009

Office of Consumer Protection
Leiopapa A Kamehameha Building
235 South Beretania Street, Suite 801
Honolulu, HI 96813

To Whom It May Concern:

We represent Network Solutions, LLC, and are writing to inform you of a data security incident involving the compromise of individuals' payment card information. Network Solutions provides e-commerce software to small and medium-sized businesses, which use the software to collect credit card-related information and transmit it to payment processors.

Network Solutions believes that, from March 12, 2009 to June 8, 2009, an unknown actor intentionally diverted certain data that passed through the Network Solutions e-commerce servers to a location outside our company. We are conducting an internal forensic investigation of this incident, and we believe that the intrusion has been contained. We have received no reports of fraud associated with this incident.

The investigation began in early June after we received reports regarding our server performance. On July 13, 2009, our forensic investigators determined that personal information in the form of credit card transaction data had been diverted out of Network Solutions systems. We contacted federal law enforcement authorities regarding the incident within 48 hours of that determination and are cooperating fully with their investigation. Our forensic team continued their work to help us determine the scope of the incident, as well as the specific merchants and card holders who might have been impacted. Based on the results of our investigation thus far, we believe that the data at risk consists of cardholder names; shipping and/or billing addresses; and credit card account numbers, security codes such as CVV codes, and expiration dates.

Although Network Solutions is not the owner or licensor of the affected credit card data, we recognize that this breach is atypical in that multiple data owners are affected by the compromise. As a result, we are taking the step of notifying you directly. We have also notified payment card companies and will be notifying all three consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in 15 U.S.C. § 1681a(p)) of the incident.

RECEIVED
09 AUG -5 P2:07
STATE OF HAWAII
CONSUMER PROTECTION

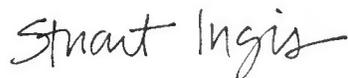
August 4, 2009

Page 2

Starting on July 24, 2009, Network Solutions notified our client merchants of this security incident. Because of the atypical nature of this incident, Network Solutions has retained TransUnion to be available to assist our affected client merchants in notifying their individual customers who may have been affected by this incident. Network Solutions will pay for 12 months of free credit monitoring for any affected consumer who is notified by TransUnion and would like to receive such monitoring. We estimate that 2,350 individuals in Hawaii will receive notification. The timing of consumer notifications will depend upon how our client merchants proceed, including the pace at which they provide necessary information to TransUnion. However, we expect that consumer notifications will begin as early as August 6, 2009. A sample copy of the notification letter that will be mailed to individual consumers by TransUnion is enclosed.

We are available to answer any questions that you may have.

Sincerely,



Stuart Ingis, Esq.

Enclosure

TransUnion c/o Network Solutions LLC
13861 Sunrise Valley Drive
Suite 300
Herndon, VA 20171

[TransUnion Logo]

[Date]

[Recipient's Name]
[Address]
[City, State, Zip (shows thru outer)]

***An Important Security and Protection Notification Follows this Cover Letter.
Please read all contents carefully.***

Dear [Insert merchant's customer name]:

TransUnion is contacting you at the request of Network Solutions LLC, a credit card software provider. The purpose of this cover note and the notification letter that follows is to alert you to a data security compromise experienced by Network Solutions that may have resulted in unauthorized access to certain information about the credit card account you used for certain transactions with one or more of its merchants.

TransUnion's only role in this matter is to:

- a) Serve as a trusted source for delivery of the accompanying notification regarding what has occurred at Network Solutions LLC
- b) Provide you with certain fraud prevention services that Network Solutions LLC has secured on your behalf, based on the circumstances outlined in the accompanying notification letter

For your own benefit, please read fully all of the details supplied by Network Solutions in the letter that follows. If you have questions after reviewing that information, please use only the contact information provided in that letter as this will help ensure that you receive the answers you need and have access to the services that have been secured on your behalf.

Sincerely,

TransUnion
Consumer Relations
P.O. Box 34012
Fullerton, CA 92834

Important Security and Protection Notification

Please read this entire letter

Dear [Cardholder Name]:

This letter is to notify you of a data security compromise that may have resulted in unauthorized access to certain information about the credit card account you used to purchase goods on a web site hosted by Network Solutions LLC. This letter also outlines the measures that are being taken – and the steps you should take – to protect your information.

First, it is important for you to understand how this occurred. In order to complete credit card transactions processed online, Network Solutions provides software services that web site merchants use to collect credit card related information and transmit to the appropriate payment processors. Network Solutions recently discovered that information on some credit card transactions, including card account numbers, names and addresses, was intentionally diverted from some of its servers to servers outside of the company by an unknown source. All cases took place between March 12, 2009 and June 8, 2009, and may have impacted approximately 4,343 merchants out of the more than 10,000 that are hosted with us. **Please note that the incident that prompted this notification to you occurred at Network Solutions.**

Upon discovering this issue, Network Solutions immediately eliminated the problem and instituted additional measures to protect its systems. **As a result, you should not be concerned that this problem has affected any transactions you may have completed after June 8, 2009, or that it might affect any transactions you intend to complete on this or other Network Solutions-hosted websites in the future.** Network Solutions has undertaken an investigation with the assistance of an outside specialist, notified law enforcement and is working closely with them on the investigation.

Your credit card information may have been diverted from Network Solutions' servers when you made the following online purchases [at (insert merchant's URL)] as indicated below:

- [Transaction Date] [Credit Card Type]
- [Transaction Date] [Credit Card Type]

The incident that caused this issue occurred at Network Solutions and was NOT a result of any actions a merchant that you purchased from may or may not have taken. The merchants who use our services do so because they know that we take your security very seriously, and are committed to maintaining best-in-class security standards. This remains Network Solutions' number one priority, and we are working with law enforcement to identify the parties responsible for this intrusion. We regret the concern and inconvenience this malicious act may have caused you.

At this point, Network Solutions has no reports or other reasons to believe that your credit card account information has been misused. Also, under established practice, your credit card issuing company generally will not hold you liable for any fraudulent purchases made using your credit card account number that are reported in a timely way to the issuer. Out of an abundance of caution, in order to help you detect the possible misuse of your information, you are being provided with the opportunity to receive one year of free credit monitoring services from TrueCredit by TransUnion. This service is completely free to you, and enrolling in the program, as explained below, will in no way impact your credit score.

**FOR MORE INFORMATION ABOUT THIS INCIDENT PLEASE VISIT
WWW.CAREANDPROTECT.COM**

What You Need To Do To Receive Your Free Credit Monitoring Services:

Go to <http://www.truecredit.com/code> and enter the following unique 16-digit gift certificate code:

- [CODE]

You can sign up for the service anytime between now and November 30, 2009. We encourage you to activate your free credit monitoring membership as soon as possible. Unfortunately, due to privacy laws, we cannot register you directly.

Following are some ADDITIONAL steps you may want to take to protect yourself against unauthorized activity on your credit card:

- Be diligent in monitoring activity on your credit card.
- If you believe that your credit card was used improperly, contact your credit card company and notify your local law enforcement and/or state attorney general. You can access information about resources at <http://www.ftc.gov/idtheft>.
- Consider obtaining your credit report. By law, you are entitled to one free credit report per year from each of the major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at <https://www.annualcreditreport.com>.
 - Equifax 1-800-525-6285 www.equifax.com
 - Experian 1-888-397-3742 www.experian.com
 - TransUnion 1-800-680-7289 www.transunion.com
- Consider notifying one of the three credit reporting companies to place a fraud alert on your file. We have already notified all three of this incident. The law allows you to place an initial fraud alert on your credit file free-of-charge for 90 days. This notification alerts creditors to follow additional procedures before opening new accounts in your name or changing existing accounts. The three nationwide credit reporting companies – Equifax, Experian, and TransUnion – are set up so that when you request an alert through one, your request is automatically sent to the other two. Generally, the alert will be placed on your credit file with all three agencies within 48 hours.

Network Solutions sincerely regrets this incident and the concern and inconvenience it may have caused you, and we encourage you to take advantage of the services outlined here. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact TransUnion at 1-800-242-5181 Monday through Friday, 8:00 a.m. to 6:30 p.m. Central Time. Please use the following 6-digit pass code, 455861, when prompted.

Respectfully,

Network Solutions LLC