

# INGENIX®

12125 Technology Drive | Eden Prairie, MN 55344 | phone: (952) 833-7100 | fax: (952) 833-7201 | [www.ingenix.com](http://www.ingenix.com)  
Mitchell W. Granberg | Senior Associate General Counsel

## VIA UPS EXPRESS

January 6, 2011

Attorney General Michael Delaney  
New Hampshire Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Dear Attorney General Delaney:

Ingenix, Inc., is writing to inform you of a possible security incident that may affect residents of your state. Ingenix hosts provider (dentist, doctor, and other medical professional) search websites for several health plans and preferred provider organizations. The websites are web-based applications that enable consumers and health plan members to search for medical providers, via the Internet. As the host of such websites, Ingenix populates the look-up tool using information that health plans and preferred provider organizations provide to it.

Ingenix has discovered that in some instances, the provider identification number provided by certain health plans contained Social Security numbers ("SSNs"). This, in turn, resulted in the potential display of a provider's name with an SSN (although the SSN would not have been identified as such) in the provider identification field for a brief time to individuals who used the provider search websites. A provider's SSN would have been displayed only for so long as the consumer query webpage was open. Our investigation of this incident, which concluded in November 2010, determined that the issue could have occurred during any point since the inception of this service, which in some cases dates back five years.

As soon as Ingenix became aware of this issue, we took prompt steps to remove the SSNs from the data used by these provider search sites and worked with the health plans to avoid a reoccurrence of the error.

On December 29, 2010, we began making written notification via USPS to 142 New Hampshire providers who may be potentially affected by this incident. A copy of the template notice letter that we sent to providers is enclosed.

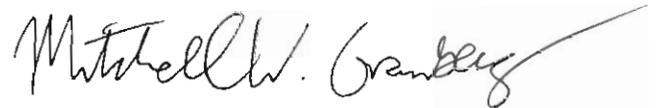
Ingenix takes matters such as this very seriously. Based on our investigation, it was determined that no other sensitive information besides SSNs was potentially disclosed on the provider lookup sites. There is also no evidence that any providers' SSNs were used for an unlawful purpose. However, as a precaution to help providers monitor the security of their personal information and detect any

Attorney General Michael Delaney  
January 6, 2011  
Page 2

possible misuse of personal information, Ingenix is providing a one year membership in ID Experts' identity theft protection and restoration program. The service includes a dedicated toll-free number for members of the affected population to call, a website dedicated to this event, twelve months of credit monitoring, as well as fraud restoration services and a \$20,000 insurance reimbursement component in the unlikely event that any provider experiences identity theft as a result of this incident. This membership is paid for entirely by Ingenix. Additionally, the notification letters sent to providers recommended steps providers can take to protect their identify, including informing them that they should report suspected incidents of identity theft to local law enforcement or the attorney general. It also explains to them how to place a fraud alert and/or security freeze on their credit file and provides them with the contact information for the national credit reporting agencies and the Federal Trade Commission.

Please note that Ingenix is providing this notification on behalf of its health plan and preferred provider organization customers as it receives approval to do so. Do not hesitate to contact us if you have any questions about this incident.

Sincerely,

A handwritten signature in black ink that reads "Mitchell W. Granberg". The signature is fluid and cursive, with a long, sweeping underline that extends to the right.

Mitchell W. Granberg  
Senior Associate General Counsel

Enclosure

PO Box 2444  
Faribault, MN 55021-9144



NAME  
ADDRESS LINE 1  
ADDRESS LINE 2  
CITY, STATE, ZIP CODE

To Enroll, Please Call:  
1-877-225-9893  
Or Visit: [www.ClinicianNotification.com](http://www.ClinicianNotification.com)  
Your Access Code: [Code]

MONTH XX, 2010

Dear NAME,

We are writing on behalf of our client, Ingenix, Inc., to inform you of the possible disclosure of your Social Security number, and of the steps that have been taken to correct the issue and protect the security of your personal information.

As a medical professional, you are aware that many health plans and health insurance brokers maintain "provider search" websites that allow patients to search for medical services. Ingenix, who hosts such websites for several health plans and brokers, learned that the "provider identification number" provided by one or more health plans and displayed during some specific provider searches was your Social Security number.

The number displayed was not labeled as a Social Security number, but rather appeared as a provider ID or similar designation. It also appeared only when your information matched a specific patient query and was often mixed with other types of provider IDs across multipage results. Therefore, it would not have been obvious to the viewer that it was a Social Security number. It would have been displayed only for so long as the patient query webpage was open.

While our client found this occurrence to be relatively rare overall, the disclosure could have occurred during any point since the inception of this service, which in some cases dates back five years. You should note that this issue does not concern your patients' personal health information or any other of your personal or financial information.

As soon as Ingenix became aware of this issue, it promptly took steps to remove the Social Security numbers from the data used by these provider search sites, and undertook an investigation to determine which medical professionals may have been affected. In addition, it worked with the health plans to help avoid a reoccurrence of the error. While there is no evidence to suggest that your information was used for any improper purpose, our client would like to offer you a 12-month subscription to ID Experts® FraudStop™ credit monitoring and recovery services at no charge to help ensure the security of your personal information.

ID Experts is an independent contractor and service provider for data disclosure response services to healthcare organizations across the United States.

Enclosed are instructions for registering with ID Experts. Please call 1-877-225-9893 if you have questions.

Regards,

**The ID Experts Team**

## Recommended Steps to Protect Your Identity

**Please Note: No one is allowed to place a fraud alert on your credit report except for you, please follow the instructions below to place the alert.**

Ingenix has contracted with ID Experts® to provide you with FraudStop™ identity monitoring and recovery services to help protect your identity. Your one year membership will include the following:

- **Fraud Resolution Representatives:** ID Experts will provide assistance if you suspect that your personal information is being misused. A recovery advocate will be assigned to your case, and they will work with you to assess, stop, and reverse any fraudulent activity. If you suspect or discover suspicious activity, you should contact them immediately for assistance.
- **Credit Monitoring:** ID Experts will provide 12 months of credit monitoring that will notify you by email of key changes in your credit file. Credit monitoring is included as part of your ID Experts membership, but *you must activate it for it to be effective*. Detailed instructions for activating your credit monitoring are provided on the ID Experts member website which you may log into once you enroll.
- **Exclusive Educational Materials:** The ID Experts website includes a wealth of useful information, including instructive articles, a Protection Test that you can take, very helpful ID Self-Defense Academy™ and a place where you can review and update your account. Their experts will keep you up-to-date on new identity theft scams, tips for protection, legislative updates and other topics associated with maintaining the health of your identity.
- **Insurance Reimbursement:** ID Experts will arrange \$20,000 of identity theft reimbursements for certain expenses that can be incurred when resolving an identity theft situation.

By immediately taking the following simple steps, you can help prevent your information from being misused.

**1. Telephone:** Contact ID Experts at 1-877-225-9893 to gain additional information about this event and to talk with knowledgeable people about appropriate steps to take to protect your credit record. Representatives from ID Experts are available to assist with enrollment in the program Monday through Friday from 8 am-8 pm Central Time.

**2. Website:** Go to [www.ClinicianNotification.com](http://www.ClinicianNotification.com) and follow the instructions for enrollment. If you do not have Internet access, you can also call 1-877-225-9893 to enroll over the phone. Once you have completed your enrollment, you will receive a welcome letter either by mail or by email if you provide an email address when you sign up. The welcome letter will detail the components of your membership and it will also contain instructions for activating your credit monitoring. It will direct you to the exclusive ID Experts' Member Website where you will find other valuable educational information

**3. Activate the credit monitoring** provided as part of your membership with ID Experts, which is paid for by Ingenix. Credit monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have access to a computer and the Internet to use this service. The welcome letter you receive after enrolling will provide you with instructions and information to activate the credit monitoring portion of the service. If you need assistance, ID Experts will assist you. They can be reached at 1-877-225-9893.

With credit monitoring, you will receive notification within 24 hours of critical changes to your credit report. You will quickly find out about changes, including potentially fraudulent activity such as new inquiries, new accounts, late payments, and more.

**4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. You can receive free credit reports by placing fraud alerts and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months

If you discover any suspicious items and have enrolled with ID Experts, notify them immediately by calling or by visiting their Member website and filing a theft report.

If you file a theft report with ID Experts, you will be contacted by a member of the Recovery Department who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Experts Recovery Advocate who will work on your behalf to identify, stop, and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**5. Place Fraud Alerts** with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's website. If you elect to participate in the credit monitoring as discussed above in #3, ***please wait until after*** you have activated the credit monitoring before placing any fraud alerts. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

#### Credit Bureaus

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

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

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

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

**6. Security Freeze:** By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze is no more than \$10 for each credit reporting bureau for a total of \$30. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the Federal Trade Commission, there is no charge to place the freeze.

**7. You can obtain additional information** about the steps you can take to avoid identity theft from the following:

**For Maryland Residents:**

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

**For North Carolina Residents:**

Office of the Attorney General of North  
Carolina  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
[www.ncdoj.com/](http://www.ncdoj.com/)  
Toll Free 1-919-716-6400

**For all other US Residents:**

Identity Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)  
1-877-IDTHEFT (438-4338)  
TDD: 1-202-326-2502