



## **Frequently Asked Questions – Security Breach**

### **How and when did this happen?**

This was a sophisticated, illegal attack into our website through a third-party vendor's software. We are working with local authorities on the investigation of the security breach. The illegal hacking occurred initially on September 22 and took place over several days. The initial interpretation was thought to be problems caused by typical computer viruses. Once confirmed that information tampering had occurred, Foothills terminated all public access websites on September 29.

### **What exactly was compromised?**

- Credit/debit card numbers and expiration date
- Card holder's name (name that appears on the card)
- Possibly the household address associated to the registration transaction.

### **Who was affected?**

Patrons who ***paid with a credit/debit card*** for the following items:

- Class registrations (conducted online at [www.foothills.org](http://www.foothills.org), in person at Foothills Park & Recreation District's facilities and over the phone)
- Rentals at the Clement Park Amphitheater
- Team registrations for activities at the Edge Ice Arena
- Player registrations for activities at the Edge Ice Arena

### **Was any other credit/debit card transactions compromised?**

No.

### **Was every single person affected who utilized the services listed above?**

No.

### **Was I affected? When will you be notifying patrons who have been affected?**

- Foothills sent out an e-mail notice on Friday, October 3 to affected patrons.
- Letters were sent between Friday, October 3 – Monday, October 6 to any affected patrons that did not provide Foothills with an e-mail address at the time they registered for a class OR if a patron had a 'bad' or 'invalid' e-mail address.

### **I haven't received an email or a letter to notify me if my information was compromised. How do I find out if I was affected?**

Please call our security hotline at 303-409-2124. If your call goes into voice mail, select option #3 and leave your name and number and a Foothills representative will return your call.

### **The last 4 digits that you sent me do not match any of my credit cards. Are you sure you sent me the correct information?**

In many cases, the card information that was compromised was from older transactions and those cards may have expired. Also, in some cases, the card information belongs to someone who may have registered on behalf of another individual. We sent notification to the household in which the registration occurred. If you need additional information about the card number reported to you, please contact us at 303-409-2124.



## **Frequently Asked Questions Continued**

### **Were social security numbers compromised?**

### **Was the three-digit security code on the back of credit/debit cards compromised?**

No. Foothills never had these pieces of information.

### **Were birthdates compromised or any other personal information for anyone under my Foothills household account compromised?**

No.

### **Why did you have my information stored?**

This has been a historical practice to retain this information to assist in the credit or refund process in the event of cancellations, drop-outs, etc. This procedure will be changing prior to the systems coming back online.

### **Why did you wait so long to let people know? Why didn't you act sooner?**

Foothills initially thought our computer system/website had been infected with a virus. We did extensive research to determine it was an illegal hacking. When we determined it was an illegal hacking, we immediately terminated all public access to our website. To determine the extent of information that was breached and which patrons were affected, it took some time to compile the information. We then immediately began notification through medial, initial e-mail notice, and patron specific e-mail notifications.

### **What other steps are you taking?**

We are in the process of doing a thorough analysis of all of our procedures and we had an independent audit of all of our network systems and registration processes. All recommendations made by the independent system consultant are in the process of being implemented and once completed, online registration will be reinstated. All credit card transactions will be handled by an outside, credit card processing company that specifically provides this secure service.

### **Will you be providing credit monitoring services?**

We met with several companies that provide these types of services to explore these options, but because of the number of people affected and the nature of the services offered, we have decided that we will not pursue an arrangement with a credit monitoring company. Every proposal we received included a significant focus on marketing future monitoring and reporting services to District patrons (most at a monthly cost to the patron). Because of other credit monitoring options that are available, we are not retaining a credit monitoring service.

Each of the credit bureaus will provide 90 days of free service, and our understanding is that you can ask for an extension after the 90 days have expired. If you have been a victim of fraudulent activity, we suggest that you report the activity to local authorities. If you have a police report, you can apply for credit monitoring service with Experian and they will provide this service free for seven years. We have also been informed that many of the major banks also provide credit monitoring as part of their menu of services. You may wish to inquire with the financial institution that provides your credit card or debit card services.

## **CREDIT REPORTING - FREQUENTLY ASKED QUESTIONS**

### **Does this mean that I'm a victim of identity theft?**

No. The fact that someone may have had access to your information doesn't mean you are a victim of identity theft or that they intend to use the information to commit fraud. We wanted to let you know about the incident so that you can take appropriate steps to protect yourself. The way to protect yourself is to place a fraud alert on your credit files and review your credit reports.

### **How will I know if any of my personal information was used by someone else?**

The best way to find out is to order your credit reports from the three credit bureaus: Equifax, Experian and TransUnion. If you notice accounts on your credit report that you did not open or applications for credit ("inquiries") that you did not make, these could be indications that someone else is using your personal information, without your permission.

### **What happens if I find that I have had fraudulent activity on my account?**

You should immediately notify your local law enforcement agency, contact any creditors involved and notify the credit bureaus.

### **Do I have to pay for the credit report?**

As a possible fraud victim, you are entitled to a free copy of your credit report. Simply call any one of the three credit bureaus at the numbers provided and follow the "fraud victim" instructions. You will automatically place a fraud alert on your credit file with all three of the bureaus.

- **Trans Union – 1-800-680-7289, [www.transunion.com](http://www.transunion.com)**
- **Experian – 1-888-397-3742, [www.experian.com](http://www.experian.com)**
- **Equifax – 1-800-525-6285, [www.equifax.com](http://www.equifax.com)**

You will receive a letter from each bureau confirming the fraud alert and telling you how to order a free copy of your credit report. Follow the instructions in the letters to receive your free reports.

### **What is a fraud alert?**

A fraud alert is a message that credit issuers receive when someone applies for new credit in your name. The message tells creditors that there is possible fraud associated with the account and gives them a phone number to call (yours) before issuing new credit. When you call the credit bureau fraud line, you will be asked for identifying information and will be given the opportunity to enter a phone number for creditors to call. You may want to make this your cell phone number.

### **Will a fraud alert stop me from using my credit cards?**

No. A fraud alert will not stop you from using your existing credit cards or other accounts. It may slow down your ability to get *new* credit. Its purpose is to help protect you against an identity thief trying to open credit accounts in your name. Credit issuers get a special message alerting them to the possibility of fraud. Creditors know that they should re-verify the identity of the person applying for credit.

### **How long does a fraud alert last?**

An initial fraud alert lasts 90 days. You can remove an alert by calling the credit bureaus at the phone number given on your credit report. If you want to reinstate the alert, you can do so.