



## **Northeast Credit Union Alerted that Heartland Payment Systems Inc. Experienced a Card Security Breach**

**January 22, 2009** - Northeast Credit Union is aware that Heartland Payment Systems Inc. has experienced a card security breach. Although some data was exposed, it does not mean that data related to member accounts was taken or that fraud has occurred on their account. Members can be assured that as a standard practice Northeast Credit Union actively monitors the activity on their accounts 24/7 to protect them from fraud. Members will be contacted if they need to take action.

Northeast Credit Union strongly encourages members to review their monthly statements carefully or review their account information online for daily activity by using Northeast Credit Union Home Banking and call us immediately if suspicious activity is found. It's also important for members to know that they are protected with **Visa's Zero Liability policy\***, which means Visa cardholders pay nothing for unauthorized purchases on their account. Visa reports that this incident is currently being investigated by the U.S. Secret Service.

Northeast Credit Union's Member Service Contact Center can be reached at 1-888-436-1847 and is available 24 hours a day, 7 days a week to answer questions. To further assist you, following are questions and answers regarding this card security breach and tips to prevent fraud that you might find helpful:

**Q: *Can you tell me if my Visa card information was stolen in this incident or if it has been used fraudulently?***

**A:** Although certain card account data may have been exposed, that does not necessarily mean that data related to your account was taken or that fraud has occurred or will occur on your account. Please be assured that as a standard practice Northeast Credit Union is actively monitoring the activity on your account 24/7 to protect you from fraud. We strongly encourage you to review your monthly statement carefully or review your account information online using Northeast Credit Union Home Banking and call us immediately if you see any suspicious activity. And remember that in the rare event fraud does occur, as a Visa cardholder you are protected with Visa's Zero Liability\* policy, which means you pay nothing for unauthorized purchases on your account.

**Q: *Is it only Visa cards that were compromised?***

**A:** No. Any credit or debit card that you used may have been exposed to this card security breach.

**Q: *I recently noticed fraud on my account. Is this fraud related to the recent incident?***

**A:** It is unclear whether the fraud that you reference to is related to the incident in question. It is important to know that regardless of where the fraud occurred, you are protected by Visa's

Zero Liability\* policy and as a standard practice Northeast Credit Union is actively monitoring your account 24/7 to prevent fraud.

**Q: *How did this happen?***

**A:** When your card number is used to make a purchase, the information is transmitted through the payment network. A fraudster may have gained access to your card information through one of those entities in the payment network. Please review your monthly statement carefully or review your account information online for daily activity by using Northeast Credit Union Home Banking and call Northeast Credit Union immediately if you see any suspicious activity. If you don't have Northeast Credit Union Home Banking we can register you today or call a member service representative anytime at 1.888.436.1847. While fraud resulting from data compromises is rare, it's important to understand that you're protected with Visa's Zero Liability\* policy and that Northeast Credit Union continually monitors your account 24/7 to prevent fraud from occurring.

**Q: *Has the security breach been fixed?***

**A:** Steps are being taken to make sure the exposed information is useless, and Heartland Payment Systems Inc. is working with Visa and the U.S. Secret Service to ensure no further information is exposed.

**Q: *What part of my information was stolen?***

**A:** It is too early to say if any of your information is actually at risk. It's important to note that although your information may have been exposed, it does not necessarily mean fraud has occurred on your account. As a standard practice Northeast Credit Union actively monitors the activity on your account 24/7 to protect you from fraud. Additionally, as a Visa cardholder you are protected with Visa's Zero Liability\* policy so that in the rare event fraud does occur, you pay nothing for fraudulent activity on your account. Please review your monthly statements carefully or review your account information online using Northeast Credit Union Home Banking and let us know immediately if you notice any charges to your account that you don't recognize.

**Q: *What are the chances that I become a victim of identity theft as a result of this incident?***

**A:** It is important to know that there wasn't any personally identifying information stolen, such as Social Security numbers or addresses, so we believe that the risk of identity theft is greatly reduced. In fact, fraud rarely occurs on accounts compromised during a data breach. However, it's always a good idea to check your credit report regularly for incorrect information. In fact, you're entitled to one free copy of your credit report every year at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 877.322.8228.

**Q: *If I become a victim of identity theft, how will you help to restore my good name?***

**A:** In the unlikely event you become a victim of identity theft, as a Northeast Credit Union credit card or checking account holder, you are protected by our free Identity Theft 911™ service. In addition, Visa works with the consumer network group Call for Action to provide consumers with a toll-free telephone hotline to assist identity theft victims. By calling 866.ID.HOTLINE (866.434.6854), victims can receive free and confidential assistance from trained counselors.

**Q: *What is this Identity Theft 911 service?***

**A:** The Identity Theft 911 service acts as a personal advocate that works with you from start-to-finish to restore your identity. It notifies credit bureaus, creditors and collectors, government

agencies, and relevant parties and makes all the phone calls and documentation needed to resolve your identity theft. You receive a 3-in-1 credit report, weekly credit monitoring and fraud monitoring for victims of true identity theft for a year. In addition, you receive a full year of threat alerts, proactive tips, education, and follow-up calls to avoid reoccurrence. All of these services are free to you as a Northeast Credit Union credit card or checking account member.

**Q: *What are you doing to protect my personal account information, especially in this case?***

**A:** In partnership with Visa, Northeast Credit Union offers consumers multiple layers of security protection against fraud, including Visa's Zero Liability\* policy, the ultimate protection for cardholders. With Zero Liability, consumers are not responsible for any unauthorized purchases made on their Visa cards. As a standard practice Northeast Credit Union actively monitors the activity on your account 24/7 to protect you from fraud.

**Q: *Will this affect recurring online bill payments or recurring payments debited to my account (i.e, gym dues, utility bills, etc)?***

**A:** Possibly. If your card account data was breached, then you will be issued a new Visa card and will need to update the card information where you transact your bill payments. If you pay bills through multiple merchants you might want to consider utilizing Northeast Credit Union's Home Banking to consolidate your payment at a central location.

**Q: *What can I do to ensure this doesn't happen to me again?***

**A:** While Northeast Credit Union employs the latest systems and technology to monitor and prevent card fraud, and many merchants also take the necessary precautions to protect your card information, there are some practical steps you can take to help protect yourself:

- Check your account statement promptly and immediately report any transactions that you don't recognize.
- Regularly check your account information online using Northeast Credit Union Home Banking
- Destroy all receipts before discarding them since some of them may have your card number printed on it.
- Guard your card — don't use it as collateral or give out your card number to someone on the phone, unless you initiated the call for a purchase.
- Check your credit report at least annually to ensure its accuracy.
- Register your card to use Verified by Visa and shop online with merchants that participate in the Verified by Visa service. This provides additional protection against unauthorized use of your card online.

**Q: *What should I do if I experience fraud on my account?***

**A:** Please monitor your account through both your monthly statement and online access and let us or any other financial institutions know immediately if you see unauthorized purchases. You can call Northeast Credit Union's Member Service at 1.888.436.1847.

**Q: *Are there any other tips you can provide to reduce my chances of card fraud?***

**A:** Yes. There are several actions you can take to protect your personal information. These tips are also available at [www.visa.com](http://www.visa.com).

**DO ...**

- Shred all personal and financial information — such as bills, bank statements, ATM receipts and credit card offers — before you throw it away.
- Keep your personal documentation (e.g., birth certificate, Social Security card, etc.) and your bank and credit card records in a secure place.
- Call the post office immediately if you are not receiving your mail. To get the personal information needed to use your identity, a thief can forge your signature and have your mail forwarded.
- Be aware of your surroundings when entering your Personal Identification Number (PIN) at an ATM.
- Limit the number of credit cards and other personal information that you carry in your wallet or purse.
- Report lost or stolen credit cards immediately.
- Review and consider whether you need currently inactive card accounts. Even when not being used, these accounts appear on your credit report, which is accessible to thieves. If you have applied for a credit card and have not received the card in a timely manner, immediately notify the appropriate financial institution.
- Closely monitor the expiration dates on your credit cards. Contact the credit issuer if the replacement card is not received prior to your credit card's expiration date.
- Sign all new credit cards upon receipt.
- Review your credit reports annually.
- Use passwords on your credit cards, bank accounts and phone cards. Avoid using the obvious passwords — your mother's maiden name, your birth date or the last four digits of your Social Security or phone number.
- Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.

**DON'T ...**

- Volunteer any personal information when you use your credit card.
- Give your Social Security number, credit card number or any bank account details over the phone or email unless you have initiated the call and know that the business that you are dealing with is reputable.
- Leave receipts at ATMs, bank counters or unattended gasoline pumps.
- Leave envelopes containing your credit card payments or checks in your home mailbox for postal carrier pickup.
- Record your Social Security number or passwords on paper and store them in your wallet or purse. Memorize your numbers and/or passwords.
- Disclose bank account numbers, credit card account numbers or other personal financial data on any Web site or online service location, unless you receive a secured authentication key from your provider.

**\*Visa's Zero Liability policy** covers U.S.-issued cards only and does not apply to commercial credit cards, ATM transactions or PIN transactions not processed by Visa. Cardholders must notify card issuers promptly of any unauthorized use. Consult issuer for additional details or visit [www.visa.com/security](http://www.visa.com/security).