Suggested Issuer Customer Service Q&A
National Retailer Security Breach
Updated: January 11, 2014

Breach Overview

Q: Media reports are stating that Target experienced a data breach. Can you provide more specifics?

A: Yes, Target has confirmed that it experienced unauthorized access to its systems resulting in the compromise of credit and debit card information. Target has also announced that additional customer information was taken during the breach, which may include customer names, mailing addresses, phone numbers and e-mail addresses.

Although certain card account data may have been compromised in this incident that does not mean data related to your account was taken, or that fraud has occurred on your account. Please be assured that we are actively monitoring the activity on your account to protect you from fraud. You will be contacted if we see any activity that requires you to take any action.

In addition, please review your monthly and/or online statement carefully and call us back immediately if you see any suspicious activity. It's also important to note that all Visa credit and debit cards are protected with Visa's Zero Liability* policy in the rare event fraud does occur, which means you pay nothing for unauthorized purchases on your account.

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

A: Although certain card account data may have been compromised in this incident, it does not mean data related to your account was taken, or that fraud has occurred on your account. Please be assured that we are actively monitoring the activity on your account and continuing to work to protect you from fraud.

As always, please review your monthly and/or online statement carefully and call us back immediately if you see any suspicious activity. All Visa consumer credit and debit cards are protected with Visa's Zero Liability policy in the event fraud does occur, which means you pay nothing for unauthorized purchases on your account.

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

A: At this time, it is unclear whether this fraud 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. Can you provide me with more information so that I can assist you?

Q: How did this happen?

A: Target has confirmed malware on its U.S. point of sale systems resulted in unauthorized access to payment card data. The specifics in the Target case are still under investigation.

Please review your monthly and/or online statement carefully and call us back immediately if you see any suspicious activity. While fraud resulting from data compromises is uncommon, it's important to understand that you're protected with Visa's Zero Liability policy.

Q: How many cards were involved in the incident?
A: Target announced that approximately 40 million credit and debit card accounts may have been impacted between November 27 and December 15, 2013. Further, Target has also announced that additional customer information was taken during the breach, which may include customer names, mailing addresses, phone numbers and e-mail addresses for up to 70 million customers.

Q: Is it safe to shop at Target?
A: Consumers should feel safe using their Visa cards anywhere Visa is accepted.

Q: Has the security breach been fixed?
A: Yes, Target has confirmed that the breach is resolved.

Q: What part of my information was stolen?
A: Target has confirmed that the customer name, credit or debit card number, the card's expiration date, the CVV (the secret code on the magnetic stripe) and encrypted PIN information may have been compromised. Target has also announced that additional customer information was also taken during the breach, which may include customer names, mailing addresses, phone numbers and e-mail addresses.

It's important to note, though, that although your information may have been compromised, it does not necessarily mean fraud has occurred or will occur on your account. We are actively monitoring the activity on your account and working to protect you from fraud.

In the event any fraud occurs on your card, all consumer Visa credit and debit cards are protected with Visa's Zero Liability policy, which means you pay nothing for fraudulent activity on your account. Please continue to monitor your account and let us know immediately if you notice any charges to your account that you don't recognize.

Q: Is my PIN number safe?
A: According to Target, even the stolen PIN data should remain secure since it was encrypted. The PIN information was fully encrypted at the keypad, remained encrypted while it was in Target's system, and remained encrypted when it was removed from Target's system.

According to Target, it does not have the key to decrypt the PIN information within its system. The PIN information can only be decrypted when it is received by Target's external, independent payment processor. According to Target, this means that the "key" necessary to decrypt that data has never existed within Target's system and could not have been taken during this incident.

Q. What is in the new announcement from Target?
A. Target announced on January 10 that, as part of its ongoing data compromise investigation, it has learned that additional customer information – separate and distinct from the payment card data previously disclosed – was also taken during the breach. The additional data removed from Target's systems may include customer names, mailing addresses, phone numbers and e-mail addresses for up to 70 million customers.

Q. Does this mean that 70 million more accounts were compromised?
A. No. Target's announcement did not indicate that any further payment card accounts have been compromised at this time.

Phishing Scams and Consumer Protections

Q. I am worried that fraudsters may now call me since they might have my phone number.
A. Cardholders should be on high alert for suspicious calls. These calls are known as phishing calls.

Q. What is phishing?
A. Phishing refers to scams that attempt to trick consumers into revealing personal information, such as bank account numbers, passwords, payment card numbers, or Social Security numbers. These scams can be done by phone, email, regular mail and even via text message. In addition to seeking bank information, phishers may also try to obtain your ATM PIN or any other bits of data that can help them build a more complete profile from which they can operate in your name.

Most commonly, phishers target unsuspecting users with fake Internet sites or email messages that look legitimate. This is sometimes referred to as "spoofing." Scammers also may leverage social networking sites, where users are already accustomed to sharing information with others.

Q. How does phishing work?
A. Phishing emails and websites typically use familiar logos and graphics to deceive consumers into thinking the sender or website owner is a government agency, bank, retailer or other company they know or do business with. Sophisticated phishers may include misleading details, such as using the company CEO's name in the email "from" field. Another common phishing tactic is to make a link in an email (and the fake website where it leads) appear legitimate by subtly misspelling URLs or changing the ".com" to ".biz" or another easily overlooked substitution.

Some phishing scams even lure victims by telling them that their information has already been jeopardized. For example, potential victims may receive an email that appears to come from a major bank warning that their account has recently been exposed to fraudulent activity. Users are asked to click a link within the message so they can "confirm" their bank account information. Instead of going to the bank's legitimate website, however, victims are taken to a clever lookalike, where their information actually is routed to the scammer.

If you receive any message asking you to confirm account information that has been "stolen" or "lost" or encouraging you to reveal personal information in order to receive a prize, it may be a form of phishing.

It's important for consumers to know that Visa will not call or e-mail cardholders to request their personal account information, and Visa call centers do not initiate outbound telemarketing calls.

Q. How can I reduce my risk of phishing?

A. Always view any phone or email requests for financial or other personal information with suspicion, particularly any "urgent" requests. When in doubt, do not provide any information without first verifying the legitimacy of the request by calling the number printed on the back of your payment card. Find more tips for protecting yourself at www.visasecuritysense.com.

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

A: ***[DISCUSS ISSUER RESOURCES, OR:]***

In the unlikely event you become a victim of identity theft, 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 1(866) ID-Hotline, victims can receive free and confidential assistance from trained counselors.

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

A: ***[DISCUSS ISSUER RESOURCES, OR:]***

Working with Visa, *Financial Institution Name Here* offers consumers multiple layers of security protection against fraud, including Visa's Zero Liability policy, the cardholders' ultimate protection. With Zero Liability, consumers are not responsible for any unauthorized purchases made on their Visa cards.

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

A: While we employ the latest systems and technology to monitor and prevent card fraud and merchants also take the necessary precautions to protect your card information, there are some practical steps you can take to help protect your card information:

- Shop with merchants you know. If a deal seems too good to be true, it probably is.
- Check your account statement promptly and immediately report any transactions that you don't recognize.
- Guard your card – don't use it as collateral or give out your card number to someone calling 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 – both your monthly statement and online – and let us know immediately if you see unauthorized purchases.

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.

DO...

- Be on guard for phishing scams.
- 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.
- Cancel all inactive credit 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 – such as your mother's maiden name, your birth date, and 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 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, and 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. Cardholder must notify card issuer promptly of any unauthorized use. Consult issuer for additional details or visit www.visa.com/security.