JAN 27 2014

Four steps you can take if you think your credit or debit card data was hacked

BY GAIL HILLEBRAND

Lately, we've received a lot of questions about what to do in light of the recent data breach at Target retail stores. This theft of credit and debit card information could impact tens of millions of consumers and we want to let you know what you can do to protect yourself if you spot fraudulent charges.

If your information was part of a breach, the most immediate risk is that the thieves may make unauthorized charges or debits to your accounts. Keep a close eye on your account activity and report suspicious transactions immediately to your bank or credit card provider. The sooner you tell your provider about any unauthorized debits or charges, the better off you'll be.

1. Check your accounts for unauthorized charges or debits and continue monitoring your accounts

If you have online or mobile access to your accounts, check your transactions as frequently as possible. If you receive paper statements, be sure to open them and review them closely. If your provider offers it, consider signing up for email or text alerts.

Report even small problems right away. Sometimes thieves will process a small debit or charge against your account and return to take more from your bank account or add more charges to your credit card if the first smaller debit or charge goes through. And keep paying attention—fraudulent charges to your card or fraudulent debits to your bank account might occur many months after the theft of your information during a data breach.

2. Report a suspicious charge or debit immediately

Contact your bank or card provider immediately if you suspect an unauthorized debit or charge. If a thief charges items to your account, you should cancel the card and have it replaced before more transactions come through. Even if you're not sure that PIN information was taken, consider changing your PIN just to be on the safe side.

If your physical credit card has not been lost or stolen, you're not responsible for unauthorized charges. You can protect yourself from being liable for unauthorized debit card charges by reporting those charges immediately after you find out about them or they show up on your bank statement.

If you spot a fraudulent transaction, call the card provider's toll-free customer service number immediately. Follow up with a written letter. Your monthly statement or error resolution notice will tell you how and where to report fraudulent charges or billing disputes.

When you communicate in writing, be sure to keep a copy for your records. Write down the dates you make follow-up calls and keep this information together in a file.

If your card or PIN was lost or stolen, different rules may apply. Your timeline for reporting after your card, PIN, or other access device is lost or stolen is tied to when you discover the loss or theft or when unauthorized transactions show up on your bank statement. Therefore, you should make the report as soon as you know that there is a problem

3. Submit a complaint if you have an issue with your bank or card provider s response

Debit card issuers should investigate the charges (generally within 10 business days) and take action quickly (generally within 3 business days). For your credit card, it can take longer, but you don t have to pay the charge while it s under investigation. You also have a right to see the results of their investigations.

If you have an issue with their response, you can submit a complaint online or by calling (855) 411-2372. For TTY/TDD, call (855) 729-2372.

If you have other questions about billing disputes and your debit and credit card protections, you can Ask CFPB.

4. Know when to ignore anyone contacting you to verify your account information by phone or email

This could be a common scam, often referred to as phishing, to steal your account information. Banks and credit unions never ask for account information through phone or email that they initiate. If you receive this type of contact, you should immediately call your card provider (using a customer service number that you get from a different source than the initial call or email) and report it.

For more information on phishing scams, check out the FTC s consumer alerts.

For more information, check out the consumer advisory.

1 COMMENT | CATEGORIES: CONSUMER ADVISORY | CREDIT CARDS | DEBIT CARDS | FEATURED | FRAUD | SECURITY