12/15/2014

By: Administrator

Victims of the Target data breach last year were eligible to sign up between January and April 30, 2014 for 12 months of free credit monitoring from ProtectMyID (a service of Experian). For those who enrolled early on, the free service will be ending soon. If you are one of those consumers, should you pay for a subscription for credit monitoring from ProtectMyID or from another identity theft service? It's probably not necessary.

Credit and debit card account information is only valuable to identity thieves if they can use it to make purchases themselves or if they can sell it to others for that purpose. If you changed your account numbers, the stolen numbers are of no use. Even if you didn't change them, your card issuers are probably watching for any unusual activity on your accounts and will let you know if they detect something suspicious. Many financial institutions even offer free transaction alerts so that any time your card is used, you'll be notified – ask if your card issuer provides such a service.

You can also monitor your accounts online to make sure that there are no errors or unauthorized charges or debits. Some people are reluctant to make bill payments or transfer money between accounts online, but you can still set up online access to your financial accounts in order to monitor them, even if you don't want to do anything else. Just be sure that you have good security software on the PC or mobile device that you are using to access your accounts to keep intruders out. If you're not comfortable monitoring your accounts online, at least look at the statements that are mailed to you very carefully to see if there are any questionable charges or debits.

You're not responsible for unauthorized credit card charges and your liability for unauthorized debit card use is limited, as long as you notify the card issuer as soon as you discover the problem. And card issuers have voluntary "zero liability" policies. You can also check your credit reports free once a year with each of the credit bureaus.

So chances are that if you haven't had a problem yet in connection with the Target breach, you won't, and if you do, it won't be that difficult to deal with. Of course, it's a good idea to be on guard against phishing – someone contacting you unexpectedly, pretending to be, say, Target or ProtectMyID, and asking for your personal information. If you do want to purchase identity theft services, you *will* be asked for some personal information, so make sure you are dealing with the real company. Don't click on a link in an email or provide your information to someone who calls you – find the company's phone number or website yourself and contact it directly.