Watch accounts closely when account data is hacked and report suspicious charges

Headlines about large scale data breaches can be scary, but don't panic. There are steps you can take to protect yourself.

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 card provider. The sooner you tell your provider about any unauthorized debits or charges, the better.

Tip: Watch for reports from the merchant that was hacked, or your card provider, about the nature and timing of the security breach.

Check your account statements for unauthorized charges or debits and make a habit of 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. You should do this even if you're not sure your information has been compromised.

Report even small problems right away. Sometimes thieves will process a small debit or charge against your account and return to take more if the small debit or charge goes through. Look for suspicious activity like unfamiliar merchant names, especially from merchants outside your area.

Fraudulent charges to your card or fraudulent debits to your bank account might occur months after the theft of your information during a data breach. It's important to make a habit of monitoring your accounts.

Alert your bank or card provider immediately if you think your account has suspicious debits or charges

Contact your bank or card provider immediately if you suspect an unauthorized debit or charge.

cfpb Consumer Financial Protection Bureau

Visit us online at **consumerfinance.gov**

If a thief takes money from your bank account by debit, or charges items to your credit card, you should cancel the card and have it replaced before more transactions come through. You should also consider changing your PIN just to be on the safe side.

Your best step to protect yourself from unauthorized charges or debits to your accounts is to report that your card or your information has been lost or stolen promptly after you learn of it.

For credit cards

If your account number, not your physical credit card, has been stolen, you are not responsible for unauthorized charges under federal law.

For debit cards

If an unauthorized transaction appears on your statement (but your card or PIN has not been lost or stolen), under federal law you will not be liable for the debit if you report it within 60 days after your account statement is sent to you. But if the charge goes unreported for more than 60 days, your money, and future charges by the same person, could be lost. There are timelines for the bank to investigate and recredit the missing funds to the account after you make a timely report about the problem.

The time for you to report is much shorter if your card or PIN has been lost or stolen (2 business days, in order to limit your liability to no more than $50 of unauthorized charges), so make the report as soon as you learn that your card is missing or your PIN has been stolen.

For payroll, government benefit, and prepaid cards

For these types of cards, your rights vary depending on the card. If you suspect information from a payroll, government benefit, or prepaid card was stolen, check with the provider to find out its policy and deadlines for disputing charges. Your rights vary depending on the type of card.

You can also learn more about your card protections at consumerfinance.gov/askcfpb.

How to report a suspicious charge or debit

If you spot a fraudulent transaction, call the card provider's toll-free customer service number immediately. Ask how you can follow up with a written communication. Your monthly statement or error resolution notice also likely includes instructions on 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.

Tip: If you get a replacement card, remember to update any automatic payments linked to the card.

Contact the CFPB if you have an issue with your bank or card provider's response

Card providers should investigate the charges and respond quickly – generally within 10 business days of receiving an error notice for debit card disputes or within two billing cycles for credit card disputes. You have a right to know the results of the investigation.

If you have an issue with the card provider's response, you can submit a complaint to us. Go to consumerfinance.gov/complaint or call (855) 411-CFPB (2372).

You can also learn more about billing disputes and your card protections at consumerfinance.gov/askcfpb.

Be careful of scammers! Be wary of anyone contacting you to "verify" your account information over the phone or email

If someone initiates contact with you, it 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 calls 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, visit the FTC's consumer alert page on its website consumer.ftc.gov/scam-alerts.