

Protect yourself from credit card fraud at the register

Opening a store credit card in someone's name without their permission is fraud.

Unfortunately, older consumers have told the CFPB that they received store credit cards in the mail after refusing an offer to apply for the card at the store, or over the phone.

How could this happen? These consumers may have shared their personal information, including Social Security numbers, without knowing that the cashier could use it to open a store credit card without their permission.

Don't let this happen to you.

Follow these tips for avoiding this type of fraud and protecting your credit.

Step one: Don't share your Social Security Number (SSN) unless you want to apply for new credit.

If you don't want a new credit card, don't enter your SSN into a pin pad or write it down for a store associate.

Step two: Cancel the unauthorized credit card.

If you receive a credit card that you didn't apply for, call the number on the back of the card. Explain that you didn't authorize or apply for the credit card, and tell the company to cancel it.

Step three: Report the fraud to the credit bureaus.

The credit bureaus have a responsibility to remove information about the fraudulent credit card account from your credit report after you report it. Here's how:

- **Check your credit.** Request copies of your credit reports to find out whether the unauthorized credit card is on your report. You are entitled to a free credit report from each of the three major consumer reporting companies every 12 months. Visit annualcreditreport.com. If you certify that you have reason to believe your credit report is wrong because of fraud, you can get additional free reports. Request free credit reports every year so you can spot any new fraud.
- **Dispute any inaccurate information.** If you find information about the fraudulent account in your credit report, tell the credit reporting companies that you did not authorize the store credit card. Also tell the credit card company to stop reporting the fraudulent account to the credit bureaus. Do this in writing, and be specific. Find tips to guide you through the dispute process at cfpb.gov/askcfpb.

Step four: Request a fraud alert or security freeze.

- A fraud alert requires creditors who check your credit report to take steps to verify your identity before opening a new account, issuing an additional card, or increasing the credit limit on an existing account based on a consumer's request. When you place a fraud alert on your credit report at one of the nationwide credit reporting companies, it must notify the others.
- You can also freeze your credit to prevent prospective creditors from accessing your credit report. Creditors typically won't offer you credit until you lift the freeze. So a freeze can be useful in preventing an identity thief from opening a new credit account in your name. It's free, but you must contact each credit reporting company individually. Learn more at cfpb.gov/askcfpb/1341.

Submit a complaint

It's against the law for a credit card company to issue a credit card to you without your permission. If this happens, contact the credit card company immediately. You can also submit a complaint on consumerfinance.gov, and the Bureau will work to get you a response from the company.

Contact us



Online

consumerfinance.gov



By phone

(855) 411-CFPB (2372)

(855) 729-CFPB (2372) TTY/TDD



By mail

Consumer Financial Protection Bureau
P.O. Box 2900
Clinton, IA 52733-2900