PUBLIC SAFETY BULLETIN: Credit Card Fraud Prevention

When it comes to identity theft and credit card fraud, it's more important than ever to be vigilant and take steps to protect your personal information. Over the past few years, the fraud rate has skyrocketed. According WalletHub, the total value of credit card fraud in the United States in 2024 was approximately $275 million. And the Federal Trade Commission found that credit card fraud reports increased by 7.8% from 2023 to 2024 for a total of 449,076 fraud complaints.

10 Tips to Help You Guard Your Data

The best way of detecting fraud before it gets out of hand is to keep a watchful eye on all of your accounts and credit reports. **These 10 tips can help you spend safely and guard your sensitive data:**

1. Consider a Contactless Card

Contactless credit cards look just like EMV chip cards but they dip into a sensor rather than being swiped. Contactless cards show an image of four curved lines somewhere on the card. Thes lines let you know that you can tap the card over a sensor when paying rather than inserting the card into a reader.

- Your card must be within 2 inches of the sensor to transmit the information.
- Rather than giving the merchant your credit card number, the card sends a one-time code – just like the chip.

2. Be Aware: Zero-liability Fraud Protection

Credit card issuers offer zero-liability fraud protection. That means if a fraudulent transaction appears on your account, you can alert the card issuer and follow their process for reporting the crime. You will not have to pay for purchases you did not make. Be sure to check your accounts regularly to make sure you recognize all charges.

3. Set Up Fraud Alerts to Monitor Your Accounts

Setting up alerts can help you manage your accounts and spot fraud. Alerts can typically be set on the card issuer's website or app. Sign up for automated alerts of suspicious account activity wherever offered. It may be a good idea to sign up for alerts via text and email. If an account is taken over, hackers may be able to intercept alerts sent by SMS text or phone call.

4. Alerts Can Help You Manage Your Accounts

Card issuers typically offer a number of different alert options. For instance, you can choose to get a text or email anytime a purchase is made on the card, or you can even set a purchase limit that would trigger an alert. You can also request alerts when your balance reaches a certain threshold, when you are near your limit, when the payment date is approaching – and more.

5. You May Be Able to Freeze Your Account

Some cards allow you to freeze your account for extra security. Recurring payments and rewards are still allowed to go through, plus transactions that were made before the freeze, but any new purchases are declined until you unfreeze the account. The feature can generally be activated online or through a card issuer's app, so you do not even have to speak with anyone to freeze and unfreeze your account.

6. Take Advantage of Digital Wallets

Most smartphones have a digital wallet that allows you to add your credit or debit card information. You can then use your smartphone

(or smartwatch) to pay in a brick-and-mortar store or online when retailers offer the option. Digital wallets work by transmitting a unique, random transaction number to the merchant instead of your card number. Your account information is encrypted in your digital wallet and can only be accessed via password or, with most mobile devices, your fingerprint or facial recognition. If your card information is ever lost or stolen, banks can reissue a new one immediately to your phone instead of having to wait days for a card to arrive in the mail. In addition, if you misplace or lose your phone, you can lock your digital wallet remotely. There are no fees for using digital wallets.

7. Follow Safe Online Shopping Guidelines

The first step to safe online shopping is to ensure you are shopping on a secure website. Look at the URL to find out if it's secure – it should begin with "https" not "http." The "s" indicates that the connection between your internet browser and the company's server is encrypted. You will also see a padlock icon next to the URL in your browser.

- If you set up accounts with merchants or websites, use strong passwords and do not reuse the same password across multiple sites.
- Make sure your device, whether it's a computer, phone or tablet, has the latest security updates.
- When shopping away from home on your computer, phone or tablet, avoid using public Wi-Fi to help keep your data secure.
- Consider using a credit card rather than a debit card for online shopping. Even if you do everything perfectly, you may end up shopping on a retail site that has been compromised. That could leave your bank account vulnerable.

8. Stay Safe While Traveling

It can be a good idea to call your card issuer and let them know you will be traveling away from your usual area. One way financial institutions fight fraud is by declining transactions that seem to be wildly different than your usual pattern. Calling ahead of time can help ensure that you have access to your cards. Before traveling, consider making a copy of all the cards you carry in your wallet so that you will have a list of them and the emergency phone numbers on hand.

9. Practice Good Internet Habits in General

Guarding against hackers and scammers can help keep your sensitive information safe.

- Ignore deals, freebies and awards that sound too good to be true. Disregard offers that appear to come from unusual foreign contacts, as well as requests from strangers for help.
- Ignore phone calls, emails or texts that appear to be from the IRS. The IRS will not contact you by phone, email, text message or social media to request personal or financial information.
- Be suspicious of anyone requesting your Social Security number, date of birth, financial account number, PIN, email or passwords – especially if there is a request to verify your information when you were not expecting it.
- Never click a link or download an attachment inside an unexpected email. Go to the company's website and log in to your account from there.
- Never provide personal information over the phone to an unsolicited caller. If you think the call might be legitimate, hang up and call the company directly.

10. Use All the Security Features Available and Monitor Your Data

Additional actions you can take to safeguard your information:

- Sign up for two-factor authentication (2FA) when offered.
- Make sure your financial institutions have up-to-date contact information for you, especially your mobile number.
- Check your credit report regularly.

Frank J. Mazzilli | Public Safety Manager
404.328.5246
frank@boulevardcid.org
www.boulevardcid.org

FULTON INDUSTRIAL BOULEVARD IMPROVEMENT DISTRICT