SECOND QUARTER 2025

The Credit Report

THE CARD ASSETS QUARTERLY NEWSLETTER

Credit Card Fraud Insights

As fraud numbers continue to increase, we would like to focus our entire newsletter to mitigating fraud and assisting cardholders to overcome the obstacles caused by fraudulent use of their cards.

Step One – Understanding what credit card fraud is

Credit card fraud is a crime where someone uses another person's credit card or credit card information without permission to make unauthorized transactions or purchases. This can include stealing physical cards, hacking into accounts, or using stolen card details online. The goal of the fraudster is typically to gain financial benefits at the victim's expense. The typical forms include:

- **Card Not Present Fraud**: Using stolen card details for online or phone transactions where the physical card is not required.
- **Card Skimming**: Copying card details using a device placed on ATMs or point-of-sale terminals.
- **Lost or Stolen Cards**: Physically stealing a card to make purchases.
- **Account Takeover:** Gaining access to a victim's account and changing details to use the card without consent.

Credit Card Fraud Insights Cont.

Step Two – Fraud Prevention

Preventing credit card fraud involves several key practices to protect both your personal information and your credit card details. Here are some tips to help keep your cardholders safe:

- **Use Strong Passwords**: For online banking and shopping, always use strong, unique passwords for your accounts. Avoid using easy-to-guess passwords and consider enabling two-factor authentication when possible.
- **Monitor Your Statements**: Regularly check credit card statements or transactions for any unauthorized purchases. Report any suspicious activity immediately to financial institutions or card issuers.
- **Keep Your Card Information Secure**:
  - **Never share your PIN or credit card number** over the phone, email, or online unless certain about the security of the transaction.
  - **Avoid public Wi-Fi** when making online purchases or accessing your personal account, as it can be easier for hackers to steal information.
- **Use Credit Card Alerts**: Set up transaction alerts via email or SMS, so cardholders can immediately be notified of any activity on the account.
- **Beware of Phishing Scams**: Be cautious about unsolicited emails, texts, or phone calls asking for credit card information. Financial institutions will never ask for sensitive details in this fashion.
- **Secure Devices**: Ensure that all devices have up-to-date antivirus software and firewalls to protect against malware and hacking attempts.
- **Limit the Number of Credit Cards in Use**: The fewer cards in circulation, the easier it is to monitor and manage them. It also limits the risk of multiple accounts being compromised.
- **Shred Sensitive Documents**: Shred old statements, credit card offers, or documents containing personal information to prevent identity theft.
- **Notify Financial Institutions Immediately**: If there are suspected transactions or the loss of cards, they will assist in freezing accounts and preventing further damage.

Taking these proactive steps can greatly decrease the risk of falling victim to credit card fraud.

Step 3 – Victim of Fraud?

If cardholders believe they have been a victim of credit card fraud, it is crucial to act quickly to minimize damage. The steps to take immediately are listed below.

- **Contact the Financial Institution or Card Issuer**
  - **Report the Fraud**: Call the customer service number on the back of the card to report unauthorized transactions. Most credit card companies have 24/7 fraud hotline assistance.
  - **Freeze or Cancel the Card**: Ask the financial institution to freeze the current card or cancel it and issue the new one. This will prevent further fraudulent charges.
  - **Dispute Unauthorized Transactions**: Start the process of disputing any fraudulent charges and request a chargeback for the transactions.
- **Review Statements**
  - Check All Transactions: Go through recent credit card statements or online account to identify any other unauthorized transactions.

Credit Card Fraud Insights Cont.

- **File a Police Report**
  - **Report the Fraud**: Depending on your location, the police report may be needed for identity theft or fraud. This can be used as proof of a crime for legal or insurance purposes.
- **File with the Federal Trade Commission**
  - **Report the Fraud**: If cardholders are in the US, file a report with the FTC at IdentityTheft.gov. This serves as the official record of the fraud case.
- **Place a Fraud Alert or Credit Freeze**
  - **Fraud Alert**: Place a fraud alert on credit report.
    - Place a Fraud Alert - Experian
    - Identity Theft Information: Guide to ID & Credit Fraud | Equifax
    - Fraud Victim Resources | TransUnion
  - **Credit Freeze**: Cardholders can place a freeze on their credit preventing new accounts from being opened without permission
    - Freeze or Unfreeze Your Credit File for Free - Experian
    - Security Freeze | Freeze or Unfreeze Your Credit | Equifax®
    - Credit Freeze | Freeze My Credit | TransUnion
- **Check Credit Reports**
  - **Obtain Free Credit Report**: Cardholders can request a free credit report annually from each of the major credit bureaus via Annual Credit Report.com - Home Page to check for any unusual activity or accounts.
  - **Monitor for New Activity**: Monitor for any changes such as new inquiries, accounts, or addresses.
- **Change Passwords and PINs**
  - **Update Online Accounts**: Change account passwords and shopping accounts. Use strong, unique passwords and enable two-factor authentication if possible.
  - **Reset PIN**: If there a possible compromised PIN, change the number immediately.
- **Keep Documentation**
  - **Track Everything**: Keep record of all communication with the financial institution, police, and other relevant parties.Include reference numbers, emails, or any additional documents related to the fraud case.
- **Monitor Accounts**
  - **Ongoing Monitoring**: Regularly monitor statements and credit reports for any new signs of fraud.
- **Be Cautious of Scams**
  - **Avoid Phishing Attempt**s: After reporting fraud, be aware that scammers may target people, pretending to be from financial institutions and other agencies. Verify authenticity of any communication before responding.
- **Consider Identity Theft Protection**
  - **Enroll in Monitoring Services**: If concerned about long-term effects of identity theft, consider signing up for identity theft protection services that help monitor personal information across multiple platforms.

By taking these steps, cardholders can minimize the impact of credit card fraud and better protect from future incidents.

Credit Card Fraud Insights Cont.

Latest Financial Scams

To assist in protecting cardholders, knowledge is key. Awareness of the common financial scams will assist in recognizing susceptible individuals and help those individuals overcome their obstacles. We have compiled a list of the common scams below for you.

- **Phishing Scams**: Fraudsters send fake emails or texts pretending to be legitimate businesses, such as banks or government agencies to steal sensitive information like login credentials or financial data.
- **Investment Scams**: Fraudsters promise high returns with little to no risk. These may include fake cryptocurrency investments, Ponzi schemes, or “too good to be true” stock tips.
- **Romance Scams**: Scammers target individuals on dating platforms, creating fake emotional connections to persuade them to send money, often under false pretenses.
- **Tech Support Scams**: Scammers pose as tech support representatives, claiming your computer has a virus or security issue, and then charge for unnecessary services or steal personal data.
- **IRS or Tax Scams**: Scammers impersonate tax authorities like the IRS, threatening victims with fines or arrest unless immediate payments are made, often via wire transfer or gift cards.
- **Lottery or Prize Scams**: Victims are told they have won a lottery or prize but must pay fees or taxes upfront to claim their winnings.
- **Credit Repair or Debt Relief Scams**: Scammers promise to fix bad credit or eliminate debt, but instead, they collect fees upfront and offer little to no help.
- **Business Email Compromise**: Attackers hack or impersonate legitimate business emails to trick employees into transferring funds or sharing sensitive data.
- **Charity Scams**: Fraudsters exploit goodwill by posing as charitable organizations, especially during times of crisis, to collect donations for fake causes.
- **Online Shopping Scams**: Fake online stores or auction sites offer products at unbeatable prices, only to steal money without delivering the goods.

Cardholders always need to be cautious with unsolicited communications, verify the legitimacy of requests, and do thorough research before making any financial decisions.

Please remember anyone requesting gift cards as a payment is a fraudster and communication should cease immediately.