Fraud Alert!

# Financial Fraud Update
# Prevention and Protections

- Multi-factor authentication
- Password protection
- Wi-Fi networks

Online fraud and identity theft are not going to magically disappear. We need to be thinking about protection and prevention. Here are some simple common-sense precautions that can greatly reduce the likelihood you'll be the next fraud victim.

You should use Multi-Factor Authentication, Passwords and Secure Wi-Fi Networks especially when it comes to your most sensitive data — your financial accounts and records.

## Multi-factor authentication

Multi-factor authentication (MFA) is a method of logon verification where at least two different factors of proof are required to allow an individual secure account access. *Financial Institutions have led the way and employed MFA for years.* Now other types of businesses are following. There are various types of authentication factors that are used:

- **Something you know –** includes passwords, PINs, combinations, code words. Anything that you can remember and then type, say, do, perform, or otherwise recall falls into this category.
- **Something you have –** includes all items that are physical objects, such as keys, smart phones, smart cards, and token devices.
- **Something you are –** includes any part of the human body that identifies you and can be used for logon verification, such as fingerprints, palm scanning, facial recognition, retina scans, iris scans, and voice verification.

Combine two or three factors from these categories and a multi-factor authentication is produced. Multi-factor authentication is the preferred logon verification tool.

**Takeaway:** Multi-factor authentication makes your information far more secure.

SAMPLE

## Password protection

Experts advise that you use a different password for each account and that you change your password at least twice a year for greater security. Password protection often is the last step before you access your personal information and accounts.

- **Password selection**
  Password strength is the starting point and the most important factor for you to consider before you create a password.

  Strong passwords are usually at least 10 characters long with 2 each of uppercase letters, symbols, numbers and lowercase letters. For example: P59nD#s1z*

  *Don't share your passwords with anyone.*

- **Password use**
  There's a lot to remember when you consider all the password-protected items that you use from financial accounts to home security to your refrigerator. Don't use the same password for all your accounts.

- **Password managers**
  You might consider using a reputable password management service, which will store your passwords and keep them encrypted for all your devices and accounts. A fee is often required. A web browser is not an acceptable place to store password information.

**Takeaway:** Passwords are very important to safeguarding your personal information.

## Public Wi-Fi networks

Often a public Wi-Fi network shows multiple network names that are similar. Before logon, take the time to double check that you have selected the proper network.

- **Secured network**
  Choose a secure network. Wi-Fi networks that are secure will show a lock icon next to them, or the word "secured". Often a network host/provider — whether for a conference, hotel, or coffee shop—provides you with a network for access to the internet plus a password always select a secure network.

- **Personal data and hotspots**
  If possible, avoid doing tasks like bill paying or accessing your bank account when connected to an unsecured public Wi-Fi network or hotspot. Save those transactions for when you're connected securely to your home network.

- **Virtual Private Network (VPN)**
  A VPN service uses a private link between your devices and the VPN server that encrypts your data so it's not readable. Select a top-rated service and install it on all your devices that use public Wi-Fi of any sort.

**Takeaway:** Don't mistake convenience for security.

## Additional items

- **Home Wi-Fi networks**
  Your home Wi-Fi router is the main way your devices connect to the internet. Use a strong password and name the router so that it's not apparent it's in your home. Keep the router software up to date.

SAMPLE

- **Personal information**
  Remember that your personal information is unique and private — be wary of any email, letter or telephone call asking you to confirm your personal information or pay to solve a personal account problem — it's probably attempted fraud.

- **Fraud techniques**
  A major change in the cyber-fraud methods occurred when hackers began to breach massive amounts of personal data from retailers, healthcare insurers and even credit reporting companies. Now there is targeted phishing, targeted texting, targeted pop-up windows even targeted telephone calls that use pieces of personal information to gain your trust. The true intent of this targeting is to trick you into revealing your personal financial information including user ids and your passwords.

## Resources

- Federal Trade Commission
  **www.ftc.gov**
- Identity Theft Resource Center
  **www.idtheftcenter.org**
- Financial Fraud Enforcement Task Force
  **www.stopfraud.gov**

SAMPLE

© FINANCIAL EDUCATION CORPORATION