Fraud and Scam Prevention

Bad actors continue to create new schemes designed to defraud people and are now using Artificial Intelligence to their advantage. Knowing what to look for and how to protect yourself could prevent serious financial loss at the hands of scammers.

Common Scam Scenarios

- A **tech support** "representative" informs you of supposed computer problems and requests you send them money or grant them access to your computer.
- "Representatives" from **government agencies** such as the IRS, FBI, FTC, Social Security Administration, or other officials indicate you must take action immediately to resolve an issue.
- An online **romantic interest** sends urgent requests for you to send funds via money transfers, gift cards, or cryptocurrency to address a made-up story or need.
- You receive a text or social media message from someone encouraging you to send money for an **investment opportunity**. The scammer often shows "proof" of the returns via a fabricated online portal.
- Someone claiming to be a **relative or friend** calls with an urgent problem that can only be solved if you send money. For example, a scammer poses as your grandchild who needs money to get out of jail.

Signs of Fraud

- **Unsolicited requests:** Be cautious of unsolicited emails, phone calls, or messages asking for personal or financial information. Links and phone numbers are easily spoofed so reach out to the organization directly using official contact information.
- **Urgency and pressure:** Fraudsters often create a false sense of urgency, pressuring you to make quick decisions without proper verification. Delay does no harm so take time to think about the legitimacy of the request before responding or acting.
- **Too good to be true offers:** Be wary of promises of high returns with minimal risk. A legitimate investment opportunity will provide paperwork and disclosures to open an account in your name.
- **Requests to transfer money:** Financial institutions and law enforcement agencies will never ask you to transfer money out of your account as a safety measure, or to withdraw your funds in order to purchase gift cards, cryptocurrency, gold, or other assets.
- **Demand for secrecy:** Scammers often tell you to keep the conversation secret from your loved ones and the police, claiming it's necessary to protect your family, the investigation, or your money. Real representatives of a financial institution or law enforcement agency will never ask you to keep quiet.
- **Threats of legal action:** If someone says you may forfeit an account, face a lawsuit or judgment, or be subject to a fine or arrest, be very skeptical. A resolution to these issues will never require you to move money for "safekeeping."
- **Giving you a script:** To avoid raising red flags when completing a money movement request, fraudsters may coach you on what to say to a financial institution or offer to stay on a chat while you call your bank.

Steps to take if you think you have been the victim of fraud:

- Cease communication with the bad actor
- Contact Davenport and other financial institutions to report the problem
- Change email and online account passwords
- Consider opening new accounts if your account numbers were compromised
- Contact the three credit bureaus to place a fraud alert or freeze on your credit reports
  - Equifax: 800-685-1111
  - Experian: 888-397-3742
  - TransUnion: 888-909-8872
- File a report with your local police department
- File a complaint with the Internet Crime Complaint Center
- Report phone calls or text messages to the Federal Trade Commission at 877-382-4357
- Monitor you accounts for suspicious activity and contact your financial institution if needed