The rise in popularity of Artificial Intelligence (AI) and Machine Learning (ML) has created a new generation of cyber threats and scams called Deepfake Scams. The last several months have seen a rise in deepfake scams in the financial sector, and it does have the potential to impact EagleBank customers.

What is Deepfake?

Deepfakes manipulate text, video, audio, and images for malicious purposes, utilizing AI/ML to create believable and highly realistic but entirely fabricated audio and video content. Deepfakes therefore are synthetic media named for the deep-learning methods used in the creation process and the fake events they depict.

What are Deepfake Scams?

Scammers use this technology to impersonate trusted individuals, such as bank representatives, government officials, or even your friends and family members. They then exploit these impersonations to deceive individuals into divulging sensitive financial information or making fraudulent transactions.

How to Detect Deepfakes:

- Pay attention to inconsistencies in facial expressions, lip-syncing, or eye movements. Deepfake videos may have subtle irregularities that you wouldn't see in genuine recordings.
- Listen closely to the audio for any unnatural changes in tone or quality. Deepfake audio may sound slightly robotic or have anomalies.
- Verify the authenticity of the communication by cross-referencing information with trusted sources or contacting the supposed sender through a known, public, or secure channel.

How to Protect Yourself:

- **Verify the Source:** Always verify the identity of the person or organization you're dealing with, especially if you receive unsolicited communication. If you're unsure about the legitimacy of a request, contact the institution directly.
- **Be Skeptical:** Exercise caution when receiving unexpected requests for sensitive financial information or urgent actions. Deepfake scams often rely on creating a sense of urgency or exploiting emotions to manipulate victims. Trust your instincts and question any unusual requests – especially if they seem too good to be true or hard to believe.
- **Stay Informed:** Stay up to date on the latest developments in deepfake technology and common tactics used by scammers. Awareness is key!
- **Protect Your Personal Information:** Never share your account credentials, PINs, or other sensitive information with anyone, especially over the phone or via email. Legitimate financial institutions will never ask you to provide this information unsolicited.
- **Report Suspicious Activity**: If you suspect that you've been targeted by a deepfake scam or have encountered fraudulent activity, report it to your financial institution immediately. Prompt reporting can help prevent further harm and protect other customers.
- **Educate Yourself:** There is a lot of information on deepfakes on the Internet. We found these valuable:
    - The NSA, the FBI and DHS/CISA produced a report, "Contextualizing Deepfake Threats to Organizations" on the rapidly increasing threat from developing technologies to banks and other large-scale U.S. infrastructure (September 2023).
    - ABCNews segment (November 2023).

Our Commitment to Your Security:

At EagleBank, we have robust security measures in place to safeguard your accounts and personal information. However, it is important to empower our customers to protect themselves against emerging threats like deepfake scams. By working together, we can create a safer banking environment for everyone.

If you have any questions or concerns about deepfake scams or other security-related matters, call us at 301.986.1800 or by email at ContactMe@EagleBankCorp.com. We are here to help.