ACH FRAUD ALERT FOR BUSINESSES

In recent weeks, the Bank has seen a rise in fraudulent ACH activities where businesses have had their computers attacked with malware that is able to detect business account and login information. The attackers then use this information to originate multiple ACH transactions sending money from the business account to individuals around the country. The individuals then forward the proceeds offshore for a fee. This is happening at all banks and losses are mounting across the country.

Some of the common elements that we have seen in these schemes are as follows:

- The attacks are on small to medium size businesses (the attackers believe these businesses have less sophisticated detection software).
- Malware is inadvertently downloaded to the business computer when someone in the business (usually someone who initiates funds transfers) opens an email that contains an infected file or a link to an infectious website.
- The companies have no idea that their computers have been compromised until the fraud is detected.
- The ACH files are created for an amount similar to what the business normally processes and the credit transactions to individuals are in amounts that range from $2,000 to $10,000.

DON'T BECOME A VICTIM!

Consider some of the following practices to protect your business:

- Set up a computer that is dedicated strictly to online banking activity that is not used for receiving e-mails or general internet browsing
- Limit or eliminate unnecessary web-surfing and/or email activity by employees
- Reconcile your account on a daily basis to detect unauthorized transactions
- Immediately review Wire, ACH or other transaction confirmations
- Do not use the same login or password on any other website or software
- Never share user IDs, passwords, or PIN numbers with anyone
- Never leave your workstation unattended while logged into a secure website
- Consider changing passwords every 90 days
- Have your IT staff thoroughly and routinely check your computers for viruses, trojans,, worms and other forms of malware.
- Install and keep your anti-virus, anti-malware and anti-spyware programs updated
- Consider installation of a firewall and make sure it is active and automatically updated
- Contact your insurance agent to see if you can purchase insurance protection for losses resulting from computer intrusions
- If you have suspicious activity on your account you should contact the Bank immediately