Bank of Utica

222 Genesee Street
Utica, New York 13502

www.bankofutica.com
Visit us on Facebook!

Understanding ACH Payment Fraud—what it looks like and how to prevent it.

If you've ever transferred money from one bank to another, you've probably heard of the Automated Clearing House (ACH) network. While ACH payments (like the direct deposit of your payroll or an online bill payment) are generally safe and convenient, they are—like any other method of transferring funds—susceptible to fraud. Some common types of ACH payment fraud include:

- **Phishing & Malware:** Criminals steal banking credentials through fake emails or, in some cases, installing malicious software to capture data, and then unauthorized withdrawals are initiated from victim accounts.
- **Business Email Compromise:** Attackers impersonate executives or vendors to trick employees into initiating fraudulent ACH transfers.
- Businesses also have to keep an eye out for insider threats like employees with access to financial systems that may initiate fraudulent payments.

Mitigating the risk of ACH fraud starts with regularly reviewing your bank statements, staying aware of the latest fraud tactics and minimizing possible vulnerabilities by:

- Creating strong passwords—try to use unique and complex passwords
- Do not click links or download attachments in unsolicited messages
- Keep software, firewalls, and antivirus protection up to date
- Sign up for free Real Time Alerts in Online Banking

Businesses can expand their fraud protection by implementing dual-control approvals for transactions or utilizing our **Positive Pay** services to pre-authorize or filter outgoing ACH debits, rejecting any that do not match established criteria. Call our Personal Banking Department for more information.

Information:
315-797-2700

Checking:
315-797-2761

24-Hour Banking:
315-797-2710

Toll Free:
800-442-1028

Fax:
315-797-2707