Treasury Management

Quarterly Newsletter

Legence® Bank Member FDIC

What's Inside:

Message from Legence Bank

At Legence Bank, we believe our purpose is to make our communities stronger and better – helping individuals, families, businesses, and farmers achieve financial success. To ensure we are delivering these standards, we will be providing resources in a quarterly newsletter to help YOU!

Legence Bank is committed to bringing you the best in personalized services, resources and solutions to your financial needs. As always, our team is available to answer questions. We appreciate YOU and value your commitment to banking with Legence.

Meet Our Team

Treasury Management Department

Matt Simmons
Business Support Specialist

Office: (618) 658-3249
Cell: (618) 841-0513
Office Fax: (618) 658-1613
Toll Free: (800) 360-8044 (3249)
Email: msimmons@legencebank.com

Allison Browning
Treasury Management Specialist

Office: (618) 658-3254
Office Fax: (618) 745-5228
Toll Free: (800) 360-8044 (3254)
Email: abrowning@legencebank.com

Education for ACH Originators

by Jen Kirk
AAP, Vice President, Education, EPCOR

If you are a business that originates ACH payments, the ACH Rules likely feel overwhelming. However, it's extremely important that you, as an Originator, understand and abide by the ACH Rules. Luckily, there are several ways you can understand your responsibilities without breaking much of a sweat. Here are some of the resources EPCOR's payments experts have created for businesses like yours, to make ACH Rules compliance a little easier.

ACH Rules

Keeping the ACH Rules at your Originating fingertips is a great way to make sure you have access to the information you need for on-the-spot decision making. The Rules are available in a paper copy, App version or Online version. We also have ACH Quick Reference Cards for Corporate Users to help Originators find quick information on ACH Returns, Dishonored Returns, Standard Entry Class (SEC) codes, Transaction codes and Notifications of Change (NOC).

ACH Quick Reference Guide for Corporate Users

Next year, we're rolling out a brand-new resource we're calling the ACH Quick Reference Guide for Corporate Users. This Guide is a quick summary of all the ACH Rules that ACH Originators need to know, and covers general rules, ODFI/Originator requirements, pre-requisites, and warranties, as well as a review of all the processes such as returns, NOCs, prenotes and more! This new resource will be available for as low as $30 and will be available in both print and electronic versions. We can't wait to hear what you think!

Annual ACH Rules Update (for Corporate Users)

Each year, our training team puts together this handy document that outlines ONLY the ACH Rules changes that pertain to corporate users in the coming year. We break those changes down in easy-to-understand language and explain their impact on corporate users—from their perspective. This update is part of our April edition of Payments Insider each year.

Be sure to take advantage of the resources above and remember, your financial institution is there to help.

Don't Get Smoked with Counterfeit Check Scams

by Cheri Fahrbach
Senior VP& Manager, Retail Banking, First National Bank & Marcy Cauthon, AAP, APRP, NCP, Director, On-Demand Education, EPCOR

Picture this—a gentleman has extensive smoke damage to his home due to an electrical fire. This information was posted on social media and shortly thereafter, he began receiving messages from a woman who appeared compassionate about his situation and willing to lend an ear. After sending one photo of herself and a brief Skype phone call, money became a point of conversation.

The woman claimed to have funds due to her from an estate that her "uncle," was helping her access. In the end, the man sent $5,000 to help this woman with attorney fees, thinking he was assisting her in collecting her inheritance so she could fly overseas to see him.

Just his luck—the woman had a friend in construction, so she offered to provide funds to the man in the amount of $60,000 for home repairs. He was dealing with extensive smoke damage, after all. He was instructed to open an IRA, then do an early withdrawal and take a cashier's check for $47,000 to the woman's friend's financial institution, which he did. In the end, because the teller at the financial institution of first deposit put a hold on the funds, the man and the financial institution were spared losing $47,000.

Believe it or not, situations like this involving counterfeit checks and similar frauds are all too common. Typically, a person will receive a check from a scammer for a variety of reasons. They're told they are a sweepstakes winner, or they have received overpayment for online purchases, or it's pay from an online job to name a few. The victims are then told to use part of the funds to pay some sort of fee, taxes, charges, or other costs associated with the scam to a third party and assured they can keep most of the check for the monetary cost of the transaction. Days later, the victim discovers the check bounced at the financial institution and they are now liable for the full amount of the fraudulent check, including any money they returned to the scammer or spent themselves.

It's important to stay vigilant when fighting these types of fraudulent situations. Here are some tips for you, or for you to share with your employees and clients, to avoid counterfeit check scams:

- Do not accept a check from someone you do not know.
- Do not wire or send money to people you do not know.
- Never cash a check you are not expecting.
- Always verify a check's validity before depositing.
- Never provide any personal identifying information.
- If you receive a fraudulent check, shred the check and discard.

These scams work because fake checks generally look just like real checks, even to financial institution employees. They are often printed with the names and addresses of legitimate financial institutions, and it can take weeks for an organization to realize the check is fake. Many scammers demand that victims send money through money transfer services, like Western Union or MoneyGram, or buy gift cards and send them the PIN numbers. Once the money is wired, or scammers have the gift card PINs, it is like giving someone cash. It's almost impossible to get it back.

Focus on Fraud: A Look at Ransomware

by Jim Smith
CTP, Vice President - Treasury Management Services, Union Bank & Trust Company Source: CISA

No matter how many precautions you take to secure your company's data, you can't help but wonder if it's ever enough. If you're familiar with the evolving cyber scams, you know that education is key to helping protect your company against fraud.

Ransomware scams can be very costly and debilitating if you lose all your data or are threatened with a release of sensitive information. So, you may be asking: what is ransomware, where does it come from and how do you reduce the risk of this attack? Let's talk about it.

What is Ransomware?

Ransomware is a form of malicious software, or malware, that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data. With the rapid shift to remote work by millions of Americans, and a dramatic surge in phishing scams and fake websites, we are all at increased risk of ransomware attacks—individuals and businesses alike.

While we tend to see reports of these incidents among government and critical infrastructure organizations, this type of cybercrime can (and does) happen to any type of business or individual. Anyone connected to the internet with data stored on their device or network is at risk.

During a ransomware attack, you would likely receive messages telling you that your data has been encrypted, and demanding you pay a fee to regain access. You would then be given instructions on how to pay the fee to receive the decryption key. This "ransom" can range from a small amount to thousands or even millions of dollars, depending on the value of the data. It's usually demanded in the form of Bitcoin or other types of anonymous cryptocurrency. The cybercriminals may threaten to sell or leak this stolen data if you don't pay the ransom. They may threaten to publicly name you (or cyber-shame you) as a secondary form of extortion. The attack may also involve deleting system backups, making it even more difficult to restore your data.

Some victims pay to recover their files with no guarantee the files can be retrieved. Your stolen data may even be sold on the dark web. Recovery, when it happens, can be a difficult process that may require the services of a data recovery specialist. This process can severely impact business processes and leave organizations without crucial operational data and with a fractured reputation.

Protecting Yourself and Your Business

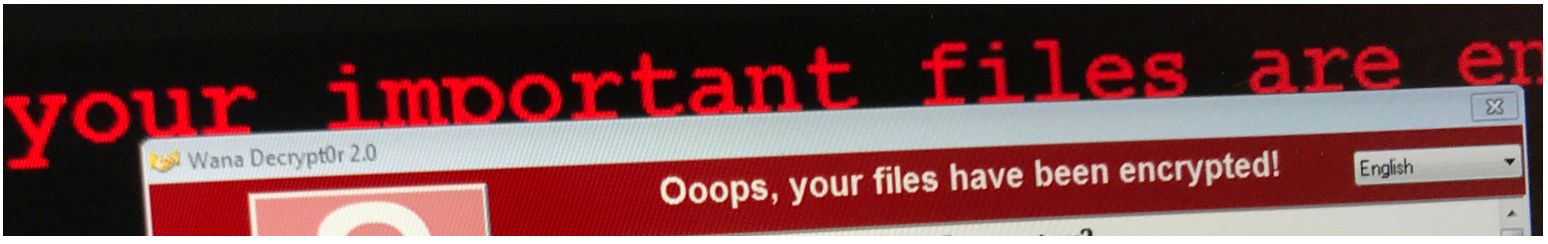
So, how do these attacks occur? And how can you prevent one from happening? This moneymaking scheme can be initiated through deceptive links in an email, instant message or a website designed to install malware.

The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following precautions to protect yourself against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails.
- Back up data on a regular basis. Keep it on a separate device and store it offline.
- Follow safe practices when using devices that connect to the Internet.

CISA also recommends organizations employ the following best practices:

- CISA released a guide for parents, teachers and school administrators that provides information to prevent or mitigate malicious cyber actors from targeting K-12 educational institutions, leading to ransomware attacks, theft of data and the disruption of learning services.
- Restrict users' permissions to install and run software applications and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application allow listing to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.



SMART BUSINESS SOLUTIONS

SMART BUSINESS CHECKING

ENJOY 1,000 free transactional items per statement cycle with the ability to add infinitely more items with low fees. In addition, we provide free online banking, bill pay, mobile deposit and access to a suite of cash management services to keep your business running smoothly. No monthly service fees allow you to keep your money where it belongs—working hard for YOU.

SMART REMOTE DEPOSIT

ENJOY depositing checks at any time without leaving your business - simply scan checks, balance, and submit. An electronic image of the check is stored and can be retrieved at anytime, so you can spend more time running your business versus running to the bank.

SMART CASH MANAGEMENT

ENJOY increased financial control without increasing your effort with the efficiency of Smart Cash Management. Banking tasks such as balance reporting, transfers, ACH origination, and more are all manageable without leaving your business. This suite of account management services is available 24/7 from anywhere with secure internet access—saving you valuable time, in addition to improving accuracy of your account information.

*Articles are provided by a semi-annual e-newsletter that is designed to inform businesses of all sizes of recent payment systems developments and is distributed in the months of April and October. Legence Bank then distributes the information quarterly.

*The EPCOR team meets and cues in a Cash & Treasury Management Committee, comprised of EPCOR members, to determine what corporate payments users need to know about current payment systems changes and challenges.

*All articles are written from the corporate user's perspective. *

If you would like a copy of the NACHA formatted rules, please contact Legence Bank

If you would like more information, please contact Legence Bank

*If you suspect a check is fraudulent, it's best to proceed with caution and reach out to Legence Bank for assistance on next steps. *