Checks and Balances

Quarterly Newsletter

Legence® Bank Member FDIC

What's Inside:

Upcoming Holidays

Christmas Day
All locations will be closed **Monday, December 26** in observance.

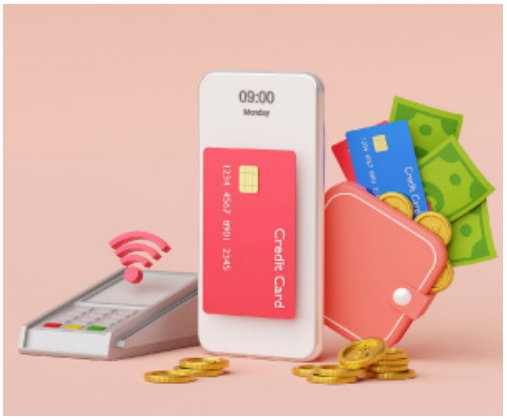
New Year's Day
All locations will be closed **Monday, January 2, 2023** in observance.

Pumpkin Spice Up Your Payments Education for 2023!

by Madison Howard
Manager, Member Communications, EPCOR

It's that time of year again—the weather is changing, the holidays are approaching and the year is quickly coming to an end. This is the time of year when many organizations begin looking ahead to the new year, make budget plans and set new goals. Plus, with many organizations seeing vital staff members approaching retirement, it's imperative to educate less tenured staff to take their place.

The best way to be successful is to have the right tools and education. So, grab your lattes and let's look at some ways to pumpkin SPICE up your payments education for your staff and clients!



ACH Rules

What better way to ensure compliance with the ACH Rules than to provide access to the ACH Rules? Consider reaching out to your financial institution if you need a copy, or additional copies.

NEW ACH Quick Reference Guide for Corporate Users

This year EPCOR rolled out a brand-new resource called the ACH Quick Reference Guide for Corporate Users. This Guide is a quick summary of all the Rules ACH Originators need to know and covers general rules, ODFI/Originator requirements, prerequisites and warranties, as well as a review of all the processes such as returns, NOCs, prenotes and more!

Did You Know... Informational Videos

These quick and free animated videos explain payments topics in just a few short minutes! The fun format and easy-to understand language make these videos perfect for passing along important information to staff and clients. Recent topics include cryptocurrency 101, cryptocurrency scams, preparing for the digital payments shift, ACH file holders and more. These videos are available on EPCOR's website, LinkedIn and YouTube channel.

Payments Insider

Payments Insider (which you're reading now) is a semi-annual e-newsletter designed to inform businesses of all sizes of recent payment systems developments. This newsletter is distributed in the months of April and October. Our April edition also includes a special ACH Rules Update for Corporate Originators. The latest copy of this newsletter is always available on the Corporate User Webpage.

Corporate User Webpage

This webpage contains end-user resources, information on upcoming ACH Rules changes and much more. And, were constantly adding new resources and taking suggestions from page visitors. Visit the webpage at epcor.org/corporateuser.

If you have any questions or aren't sure what resource is right for you or your organization, reach out to your financial institution.

Fighting the Cybersecurity Fraudsters Going Bump in the Night

by Madison Howard
Manager, Member Communications, EPCOR

Happy spooky season! If you're like me, thoughts of the fall season, comfy sweaters and scary movies are so exciting. But Freddy Krueger and the Sanderson Sisters aren't the only spooky beings to think about lurking in the shadows.

Fraudsters are always on the prowl, searching for ways to take advantage of the cybersecurity weaknesses of your organization. These fraudsters are truly monsters—which is why it makes sense that Cybersecurity Awareness Month is held in October, the epitome of the spooky season, each year.

While there's surely always something strange lurking in the cybersecurity shadows, you yourself can be a ghost (fraud) buster by implementing these cybersecurity tips and sharing them forward.

• Ditch your recycled passwords. With so many services and accounts accessible online that contain personal information, a strong password is often the only thing standing between your data and a fraudster. And, with data breaches being an unfortunately common event, it is vital to utilize new passwords and change them regularly. A strong password should contain a minimum of twelve characters (though more is better) and should not be easily guessable.

• Use two-factor or multi-factor authentication. While the extra step(s) may seem annoying, having an extra layer of protection is vital. This way, if you do fall victim to a phishing attack or data breach, you have an extra roadblock in the way of a fraudster attempting to make use of your compromised credentials.

• Keep your software up to date. Software vendors often update their products and issue patches when vulnerabilities are discovered. Sometimes these vulnerabilities are severe, with some cases being as alarming as enabling malicious third parties to completely control someone's computer without their knowledge. Its very common for fraudsters to scan the Internet for machines that are utilizing older versions of software that contain exploitable vulnerabilities. Keep an eye out for available updates and enable automatic software updates if you are able.

• Use antivirus software. There are many programs available to protect your computer from malicious code infecting your computer. This includes malware that's arrived via infected email attachments, malicious links in email messages and so-called "drive-by downloads" - automatic downloads initiated by compromised websites. Consider installing antivirus software on your electronic devices.

• Slow down! We're all busy and trying to get things marked off our to-do list as fast as possible. But slowing down before you open an email, or thinking twice before you click on a link, could be the difference between a close call and a massive data breach. Staying up to date on the latest happenings in the fraud space can help you stop fraud at the door.

What Do Third-Party Senders Need to Know About OFAC?

by Matthew T. Wade
AAP, CPA, Senior Manager, Advisory Services

As a Third-Party Sender (TPS) you may be asking, "Why do I need to be concerned about OFAC?" Or perhaps you might ask, "What does OFAC stand for anyway?" Assuming you are familiar with the acronym, you may ask, "OFAC only pertains to financial institutions, right?" Let's see if we can answer those questions for you and any others you may have.

OFAC is the Office of Foreign Assets Control and is a division of the U.S. Department of the Treasury. OFAC administers and enforces economic and trade sanctions against targeted foreign countries and regimes, and against terrorists and other individuals based on U.S. foreign policy and national security concerns. Among other things, OFAC imposes controls on financial transactions and assets of such designated parties under U.S. jurisdiction. While many OFAC policies and efforts focus on the financial banking industry, its policies and powers are not limited to financial institutions only. In fact, ALL U.S. citizens, companies located in the U.S., overseas branches of U.S. companies and, in some cases, overseas subsidiaries of U.S. companies fall under OFAC jurisdiction.

If you revisit the ACH Origination Agreement you have with your Originating Depository Financial Institution (ODFI), you may not find any explicit reference to OFAC. However, there is a good chance that somewhere in that agreement you, as a TPS, have agreed to comply with all U.S. laws. Those U.S. laws could be referring to a wide range of legislations and regulations, but assuredly, OFAC is included in the list, even if those requirements have not been specifically communicated to you by your ODFI. Many ODFIs expect their TPSs to contribute to the financial institutions OFAC program. Therefore, it is imperative that TPSs be aware of their responsibilities and their obligations related to OFAC compliance.

One common misconception is that OFAC only applies to international transactions or foreign entities or individuals. But in fact, OFAC sanctions can and sometimes do apply to U.S. citizens and companies as well. TPSs need to have policies and procedures in place to develop their own OFAC program, whether required by their ODFI or not. TPSs need to ensure they do not process or facilitate financial transactions for parties targeted by OFAC and that the proper action is taken when such transactions are presented. To make that assurance, the TPS needs to periodically scan its client base, and all parties to the transactions it processes, against OFAC's Specially Designated Nationals (SDN) list. The SDN list is a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. The list is updated frequently and is available to the public via the U.S. Department of the Treasury website. A strong OFAC program should incorporate periodic scans of the TPS's client base against the list. This can be done manually on a per-transaction basis, but there are also several automated programs available for companies to use. Your ODFI may also agree to provide this service to you or on the TPS's behalf.

Once a program is established which incorporates scans of the SDN list, the TPS should have procedures for the evaluation of "hits" and "matches" to the list, and the organization should be able to determine the difference between the two. A hit is where certain information, or strings of characters

in the information, compares favorably to a name on the SDN list. A hit could be a common surname matching individuals on the SDN list. A match is of greater quality and could be where the entire name accurately corresponds to an entry on the SDN list. With a match, there should be additional procedures to determine the validity of the match. At this point, the TPS should work with their ODFI to take the appropriate course of action.

If a valid match to a name on the SDN list has been confirmed, the TPS will need to follow OFAC procedures which could include blocking/freezing the transaction, rejecting the transaction, blocking access to funds, performing proper reporting obligations and/or discontinuing the relationship. Even with a strong program in place, consultation

with your ODFI and OFAC is highly recommended before taking any of these actions.

Hopefully, this answers some questions you have about OFAC and what it means to your organization and your participation in the ACH Network. While there is no formal requirement, having written OFAC policies and procedures is highly recommended. Another component of a strong OFAC program is the designation of an individual that is primarily responsible for the program. Finally, it is recommended that you partner

with, and seek guidance from, your ODFI in developing an appropriate OFAC program for your organization.

If you have further questions about OFAC, don't hesitate to reach out to your financial institution. If you are unsure if your current OFAC policy and procedures align with the current OFAC requirements and would like a deeper dive, contact EPCOR's Consulting/Advisory team at advisoryservicescaepcor.org! In addition to providing a comprehensive review, we can provide guidance to help you mitigate risk and improve your ACH, wire and RDC processes.

POSITIVE PAY

Get ahead of fraud with Smart POSITIVE PAY! This amazing service allows you to easily and quickly verify checks that have cleared your account with Legence Bank, ensuring they are checks you have written.

Fraud is on the rise at a rate you can't afford to not use all resources available. Smart POSITIVE PAY will help YOU identify and stop fraud in its tracks.

Partner with Legence Bank to help protect your business from fraud with Smart POSITIVE PAY!!!

FEATURES OF SMART POSITIVE PAY

- Accessible within Smart Cash Management
- Easily configure and upload check files from your current accounting/check printing software
- Receive notifications if checks don't match checks you have written
- Quick and simple notifications to Legence Bank to return items that you didn't write
- Easily identify and mark any checks that were valid written checks, but did not process properly

Business Services Department

Matt Simmons
Business Services Manager

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
Business Services Representative

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