epcor
Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

Not Reviewing Online Account Activity Daily? That's SPOOKY!

by Trevor Witchey, AAP, APRP, NCP, Senior Director, Payments Education, EPCOR

"Check your online statement at least once per day; it may help keep fraud away." Checking your online statement once a day could be your best defense against fraud's tricks! Financial institutions spend six to seven figures annually to offer you real-time statements that you can access through your internet browser or smartphone app. By reviewing these statements regularly, you can quickly spot any spooky irregularities and alert your financial institution before they turn into real nightmares!

The key to most payment systems is timing, whether it be timing to return payments or shut down an access device to prevent future fraudulent payments. Fraud happens quickly, which is why it's imperative that your organization looks at real-time account activity once per day.

Let's run through a few examples:

Unauthorized Checks—Per Reg CC and UCC 4, financial institutions may return checks within 24 hours of being presented to the paying institution. During this timeframe, your financial institution can file a breach of warranty or an indemnity request while waiting for the response of said requests.

Unauthorized Debit Card Activity—If a cardholder notices fraud on their account and contacts their financial institution immediately, the institution may close the card immediately to prevent future fraudulent payments.

Unauthorized ACH Debits—Per the *ACH Rules*, corporate debits posted to your organization's account may only be returned by your financial institution within 24 hours of the settlement date. While some ACH transaction types may have an extended return window, it's still best to review online statements daily and notify your financial institution of unauthorized transactions immediately. After realizing your organization has received a fraudulent transaction, you can also consider obtaining a new account.

Unauthorized ACH Credit/Wire Transfer Received in Error—Your organization could have tax issues if a credit that isn't yours is accepted and is spent as income. By checking accounts daily, your organization can request any credits be returned promptly.

To help catch fraud in real time, here are a few additional tips:

- Utilize the alerts component from your online platform.
- Use check or ACH positive pay ("Payee Match" is a plus for checks).
- Fraud scores from your card processor may assist with detecting unusual debit card patterns.
- Turn on wire transfer notifications for incoming wires.
- Check on FedPayments® reporting (or reporting services similar to it) for next-day ACH payment reporting.

This spooky season, keep the fraudsters in check by looking at online statements daily and receiving alerts in a timely manner! Your financial institution, and your organization's bottom line, will thank you.

What Should be Included in a Third-Party Sender's OFAC Policy?

by Matthew Wade, AAP, APRP, CPA, Senior Manager, Advisory Services, EPCOR

Anti-Money Laundering (AML), specifically the Office of Foreign Assets Control (OFAC), concerns are increasingly becoming a greater issue for third parties who engage with financial institutions in the payments space. Banking regulators are closely scrutinizing the financial institutions to determine that their relationships with third parties are not exposing the financial institutions to AML and OFAC issues. What does this mean for third parties, including ACH Third-Party Senders (TPS)? Should a TPS have an OFAC/AML policy? If so, how should that policy be constructed? Let's talk about it.

OFAC is a division of the U.S. Department of Treasury that administers and enforces economic and trade sanctions against targeted foreign countries and regimes, 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 powers are not limited to financial institutions. In fact, 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 all fall under OFAC jurisdiction.

While there is no specific requirement for a TPS to have an AML/OFAC policy, it is a recommendation often made by EPCOR. A large percentage of the third parties with whom we engage have created such a policy, and doing so exhibits the TPS's commitment to compliance with U.S. law for both domestic and international payment transactions. If you review any active ACH Origination agreements, you should find a stipulation where a TPS has agreed to comply with all U.S. laws, of which OFAC would be a part. A thorough policy is an ideal place for a TPS to start to demonstrate their organization's awareness of and commitment to the regulation.

It is recommended that the TPS's AML/OFAC policy address five essential components:

1. **Management strategy**—your organization's overall direction for AML/OFAC compliance, including allocation of resources, delegation of an AML/OFAC Officer, assignment of duties, establishment of measurement parameters and required reporting.
2. **Risk assessment**—identifying AML/OFAC risks within the TPS's activities (not just ACH) and operations. This would entail a thorough understanding of your organization's consumers, products and services, types of payments being facilitated and the geographic parameters of funds movement. The risk assessment should also seek to identify weaknesses and exposures to specific AML/OFAC risks.
3. **Internal Control**—establishing a framework for the development and implementation of specific internal controls based on the risk assessments already performed.
4. **Testing/Auditing**—internal controls, policies and procedures must be reviewed and tested periodically, and reporting of that testing should be described in the AML/OFAC policy.
5. **Training**—the policy should provide guidelines for a sufficient AML/OFAC training program for your organization and key employees.

In addition to the five components listed above, reporting and record-keeping of AML/OFAC concerns is another important topic to address in the policy. TPSs need to be aware of their responsibilities and obligations related to OFAC compliance, especially as it concerns possible restrictions on consumer activities, reporting to regulatory agencies and potentially freezing funds of which the TPS may have possession. TPSs must ensure they do not process or facilitate transactions for parties targeted by OFAC and that proper action is taken when such transactions are presented. A policy that drives compliance with these responsibilities is paramount.

Finally, the policy should establish a process to periodically scan the TPS's clients against the Specially Designated Nationals (SDN) list. The SDN list is a list of consumers and organizations owned or controlled by, or acting for or on behalf of, targeted countries. The list is updated frequently, and therefore, the client base should be compared to it at appropriate intervals. But scanning may not be the final action. In addition to the scanning process, the policy should point to detailed procedures on how the organization should proceed when there is an OFAC scan "hit".

While there is no formal requirement for a TPS to have an AML/OFAC policy, hopefully the value of creating one has become clear. The TPS's ODFI should be able to provide more guidance on AML/OFAC considerations and how your policy should be tailored to specific activities.

For any further questions about AML/OFAC and how these regulations can affect your organization, reach out to your financial institution.

Navigating the Treacherous Waters of Election Phishing Scams

In an age where information is as accessible as air, the upcoming election season has become fertile ground for fraudsters to sow seeds of deceit and misinformation. As the political atmosphere thickens with anticipation, voters find themselves bombarded with a myriad of messages, each competing for attention. However, this constant influx of political communication has an unintended consequence: it desensitizes individuals, making them more susceptible to sophisticated phishing scams cleverly disguised amidst the chaos.

The Rise of Sophisticated Scams

Election phishing scams are not a new phenomenon, but they have evolved with alarming sophistication. Techniques such as smishing, vishing, spoofing and social media phishing have become increasingly refined, making it difficult for even the most cautious individuals to discern legitimate messages from fraudulent ones.

Smishing

A text message might innocently inquire about your voting preference, masquerading as a simple poll. However, responding to such messages can inadvertently verify your phone number for fraudsters, leading to more sinister attacks down the line, including SIM hijacking or malware scams.

Vishing

Perhaps more direct, vishing involves an attacker calling potential victims and pretending to be an election official or representative from a political campaign. These calls often request personal information or financial contributions. With the ability to "spoof" caller IDs, these scammers can make their attempts appear more legitimate than ever.

Spoofing

Beyond phone numbers, the internet is rife with spoofed web pages designed to mimic official platforms. These sites lure unsuspecting visitors with promises of voter registration updates, only to steal personal information or infect devices with malware.

Social Media Phishing

Social media platforms, with their vast networks and personal connections, are prime targets for fraudsters. Fake voter registration drives, malicious donation collections and the spread of misinformation are just the tip of the iceberg.

Protecting Yourself and Your Vote

While the threat of election phishing scams is real and present, there are several steps you can take to protect your organization:

Be Skeptical

Treat unsolicited messages with caution, regardless of how benign they may appear.

Verify Legitimacy

Always verify the sender's legitimacy before responding to any requests for personal information or financial contributions.

Avoid Suspicious Links

Never click on links from unknown sources, as they could lead to malicious websites.

Use Government Sources

For any election-related information, rely solely on verified government websites.

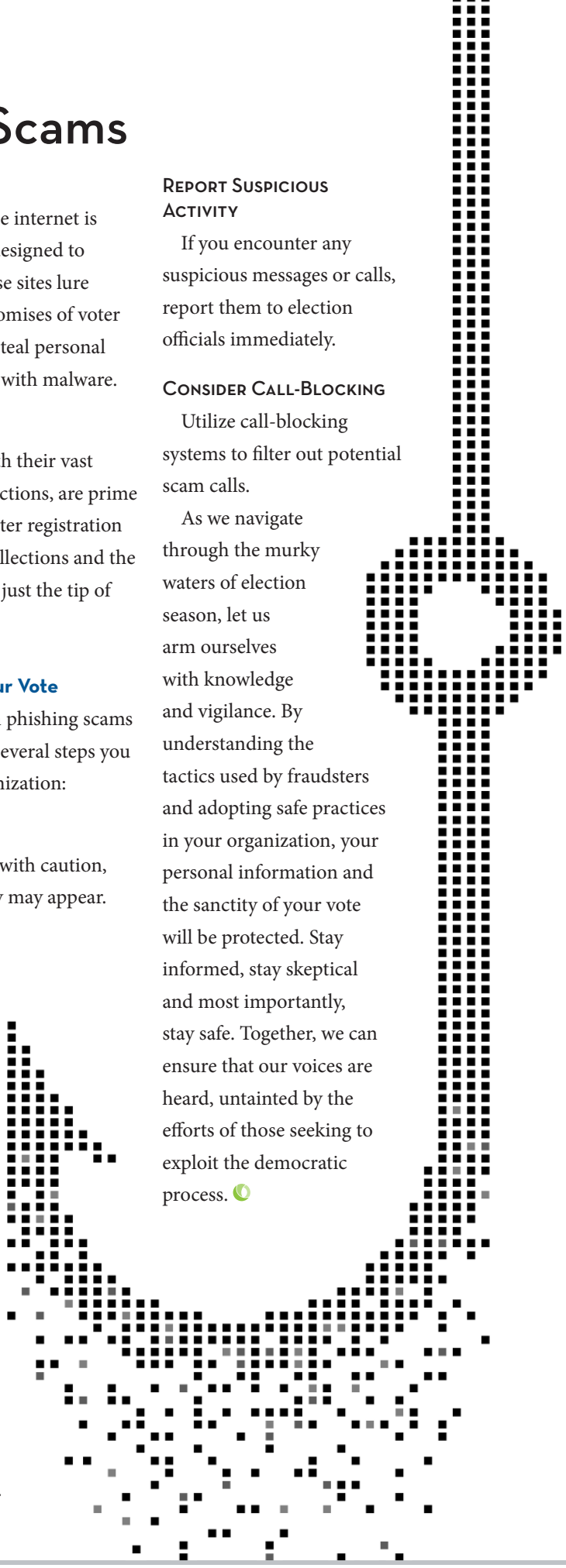
Report Suspicious Activity

If you encounter any suspicious messages or calls, report them to election officials immediately.

Consider Call-Blocking

Utilize call-blocking systems to filter out potential scam calls.

As we navigate through the murky waters of election season, let us arm ourselves with knowledge and vigilance. By understanding the tactics used by fraudsters and adopting safe practices in your organization, your personal information and the sanctity of your vote will be protected. Stay informed, stay skeptical and most importantly, stay safe. Together, we can ensure that our voices are heard, untainted by the efforts of those seeking to exploit the democratic process.



Checkmate: Defending Your Business with Positive Pay

In a world where digital payments are quickly becoming the new queen of the board, traditional check payments still play a pivotal role in business transactions. However, this reliance on checks can expose organizations to fraud—a real game of high stakes. Those who frequently rely on checks are at risk of being outmaneuvered by fraudsters, who are always ready to make their next move by producing and passing off counterfeit checks, leading to substantial financial losses.

As a responsible organization, it is imperative to take measures to stay protected from such criminal activities. So, how can your organization help mitigate check fraud? Enter positive pay—a powerful tool that enhances the security of your check transactions.

If you're unfamiliar with positive pay, it is a type of automated fraud detection technology designed to detect and prevent counterfeit checks. By leveraging this service, you can add an extra layer of security to safeguard your organization. To get started, contact your financial institution today to ask if they offer positive pay services!

Positive pay operates through a meticulous examination of checks presented for payment, comparing them against the initial company-issued checks. The system scrutinizes various check features, such as the amount, check number and payee name, to identify suspicious items or discrepancies.

Several positive pay variations can be employed, even for Automated Clearing House (ACH) transactions. Let's explore some of them:

1. **Positive Pay:** This method automatically matches each check presented against a list of issued checks provided by the organization. If any discrepancies arise, the system alerts the financial institution and the organization.
2. **Payee Positive Pay:** This approach matches the payee names from an issue file to the payee names on the check. If there is any inconsistency, the system raises an alarm.
3. **Reverse Positive Pay:** In this scenario, the financial institution sends a file of presented checks to the organization. The organization then internally compares these checks to the items they have issued, detecting any potentially fraudulent transactions.
4. **ACH Positive Pay:** This service empowers users to block and review all incoming debits or credits before they are authorized to post to an account, providing an additional layer of protection.

To shed light on the benefits of positive pay, let's explore a couple of real-life scenarios encountered by one of our EPCOR financial institution members:

Experience 1: An ex-employee of a company utilized the account information at the bottom of their payroll check to create fraudulent or counterfeit checks. The ex-employee issued these counterfeit checks to various acquaintances who subsequently cashed them at multiple branches. Unfortunately, the company had not implemented the positive pay system offered by their financial institution, and it took them several months to discover the fraud.
Total Company Loss: $4,872.39

Experience 2: A business client paid a vendor $2,800 for parts. However, during lunch break, the Accounts Receivable person left the check on their desk, allowing another vendor employee to record the MICR line information from the business client's check. This unscrupulous employee then created counterfeit checks on the business client's account to pay off their personal student loans and car loans. Fortunately, the business client had wisely opted for the positive pay service provided by XYZ Bank. This service not only verified the dollar amount and check number but also cross-referenced the payee names. Consequently, when the counterfeit checks were presented for payment, they were promptly identified as fraudulent by the positive pay system. XYZ Bank immediately contacted the business, and the counterfeit checks were returned as "counterfeit."
Total (Potential) Loss: $400,000

The second example vividly illustrates how implementing positive pay saved the business from significant financial loss. By utilizing positive pay, the business ensured advanced security for its check transactions. Although check fraud is not uncommon in the United States, organizations that heavily rely on check payments can significantly mitigate risks by leveraging protective services like positive pay.

An organization must maintain accurate records of their check payments to ensure the effectiveness of their positive pay system and prevent or minimize losses. By doing so, they can enhance the security of their bank transactions and instill peace of mind.

Take proactive steps today by contacting your financial institution to inquire about their positive pay service and determine whether its implementation is right for your organization. Safeguard against check fraud and embrace the perks of positive pay so you can say checkmate to check fraud!

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

Nacha® Direct Member

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665