



# PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

## INSIDE THIS ISSUE

|                                                                  |       |
|------------------------------------------------------------------|-------|
| 2021 ACH Rules Update for Corporate Originators .....            | pg. 1 |
| Introducing the EPCOR Corporate User Webpage.....                | pg. 1 |
| Your Role in the Reinitiation of Returned Debit Entries.....     | pg. 1 |
| No Need to Panic: A Study in Third-Party Sender ACH Audits ..... | pg. 4 |

|                                                                              |       |
|------------------------------------------------------------------------------|-------|
| Cashier's Checks: A Secure Alternative to Making a Big Cash Payment.....     | pg. 5 |
| How the Pandemic is Accelerating the Shift from Cash to Digital Options..... | pg. 6 |
| Who is EPCOR? And, Could EPCOR Membership Benefit You? .....                 | pg. 7 |
| Payment Fraud: What is it and How Can it Be Avoided? .....                   | pg. 8 |

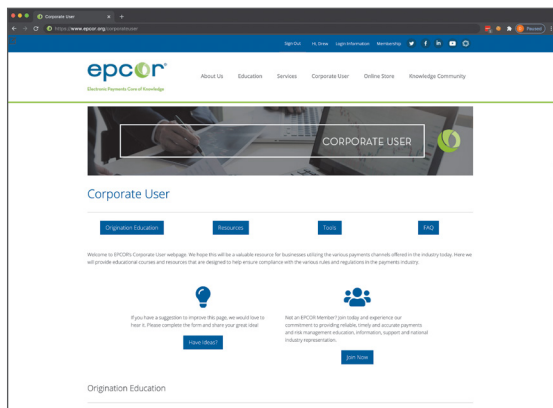
## 2021 ACH Rules Update for Corporate Originators

As an Originator of ACH entries, it is important to stay current with the *ACH Rules*, including how updates and changes might impact your business. Limitation on warranty claims, supplementing data security requirements and meaningful modernization are just a few of the changes on tap for 2021 and beyond. Get up-to-speed on these

revisions and how they will affect your organization by downloading the [2021 ACH Rules Update for Corporate Originators](#). If you have any questions about how these changes may pertain to your existing Origination activities, contact your financial institution. 

## Introducing the EPCOR Corporate User Webpage

EPCOR is excited to announce the new Corporate User webpage! EPCOR's Cash & Treasury Management Committee, consisting of financial institution and company members, identified a need for this page to assist with education for corporate



users. The site is designed to help corporate users ensure compliance with the various rules and regulations in the industry by providing educational resources. In celebration of the launch of this new

[see WEBPAGE on page 3](#)

## Your Role in the Reinitiation of Returned Debit Entries

by Liz Cone, AAP, APRP, Manager, Audit Services, EPCOR

If at first you don't succeed, try, try again. We have all heard this motivational saying, and as long as certain criteria are met, it can be applied to the Reinitiation of Returned ACH Debit Entries. One of the risks associated with the origination of ACH debit Entries is the Return of one or more of those debit Entries, which would result in a debit to the Originator's account and would require Return Rate monitoring. Should an Originator or Third-Party Sender receive a Returned debit Entry, the *ACH Rules* allow that Originator or Third-Party Sender to attempt to collect those funds two additional times. Originators or Third-Party Senders that process Reinitiated Entries should ensure staff responsible for this process understand the *Rules* that are associated with the Reinitiation of Return Entries.

[see RETURNS on page 2](#)

### When Can You Reinitiate ACH Entries?

For a Return Entry to be considered eligible for Reinitiation, one of the following criteria must be met.

- a. **No Funds Available:** The Return Entry was returned for insufficient or uncollected funds;
- b. **Stopped Payment:** The Entry was returned as payment stopped and the Reinitiation has been separately authorized by the Receiver after the Originator receives the Return Entry. For example, this could occur if a Receiver does not recognize the company name of a pending Entry and places a stop payment. If the Originator reaches out to the Receiver to provide clarification about the Entry but does not obtain a new authorization, the Entry can be Reinitiated based on confirmation of the original authorization; or
- c. **Change in Account Status:** The Originator has taken corrective action to remedy the reason for the return. An example could be an Entry being returned for Account Frozen, and the Originator has taken steps to ensure that the account is no longer frozen. This excludes Entries returned as R11.

If the Return Entry is determined to be eligible for Reinitiation, here are some other factors to keep in mind.

- a. **Reinitiation Deadline:** The Originator must Reinitiate the Entry within 180 days after the Settlement Date of the original Entry.
- b. **Maximum Number of Attempts:** An Originator may Reinitiate an Entry that has been returned a maximum of two times following the Return of the Original Entry.

### When Can't You Reinitiate Entries?

The *ACH Rules* also provide circumstances that will prohibit a Return Entry from being eligible for Reinitiation. Submitting a Reinitiated Entry that fits any of the following criteria will be considered improper Reinitiation practices.

- a. **Different Dollar Amounts:** Reinitiated Entries must be for the amount of the original Returned Entry. The Reinitiated Entry cannot be for an amount greater than or less than the original Returned Entry. If the Originator or Third-Party Sender charges a Return Fee Entry because of the Return, a separate batch with specific formatting requirements should be Transmitted.
- b. **Unauthorized Returns:** Entries returned as Unauthorized are not to be Reinitiated. A new authorization must be obtained.
- c. **Evasive Entries:** Initiating any other Entry that could be represented as an attempted evasion of the limitation on Reinitiation will also be considered improper. For example, not including "RETRY PYMT" in the Company Entry Description field in order to exceed the maximum number of attempts may be perceived as an evasive Entry.



Another piece of information important to consider is the Standard Entry Class (SEC) Code of the Return Entry. There are specific *Rules* surrounding the Reinitiation of a Re-presented Check (RCK) Entry. An RCK can only be Reinitiated if it has been returned for insufficient or uncollected funds, or the item to which the RCK Entry relates has been presented no more than one time through the check collection system, whether as a check, substitute check or image, and no more than one time as an RCK ACH Entry.

The *ACH Rules* also provide circumstances under which a debit Entry will not be treated as a Reinitiated Entry. If the debit Entry being originated in response to a Returned debit Entry meets any of the following criteria, it should not be treated as a Reinitiated Entry.

- a. **Preauthorized & Recurring Entries:** The debit Entry is one in a series of preauthorized, recurring debit Entries and is not contingent upon whether an earlier debit in the recurring series has been returned. (Example: the March debit for a loan payment is returned, and the debit Entry for the April payment is sent on schedule. The April payment is not considered a Reinitiated Entry);
- b. **New Authorization Obtained:** The Originator obtains a new authorization for the debit Entry after it receives the original Return Entry. One example could be where an Entry was returned as Unauthorized, but a new and separate authorization was obtained. Another example could be an Entry returned as stop payment, but instead of the Originator clarifying the original Entry and Reinitiating based on the original authorization, the Originator obtained a new and separate authorization from the Receiver;
- c. **Bad Account Information:** The debit Entry is initiated to the Receiver's

see RETURNS on page 3

## RETURNS continued from page 2

correct account following the return of a previous Entry using Return Reason Code R03 (No Account/Unable to Locate Account) or R04 (Invalid Account Number Structure); or

- d. **Incorrect Entry Information:** The debit Entry is initiated to the Receiver's account following the return of a previous Entry using Return Reason Code R11 (Customer Advises Entry Not in Accordance with the Terms of the Authorization), and the error or defect in the previous Entry has been corrected to conform to the terms of the original authorization in accordance with the requirements of *Subsection 2.12.5, Correction of Entries Returned as R11*.

## How do you Reinitiate Entries?

Now that it's been determined the Return Entry is eligible to be Reinitiated, it is important to ensure that the Reinitiated Entry is formatted in accordance with *ACH Rules*

requirements. The Originator or Third-Party Sender must submit Reinitiated Entries as a separate batch containing the word "RETRY PYMT" in the Company Entry Description field of the Company/Batch Header Record. The description "RETRY PYMT" must replace the original content of the Company Entry Description field transmitted in the original Entry, including content otherwise required by *ACH Rules*.

The Company Name, Company Identification and Amount fields of the Reinitiated Entry must be identical to the contents of the original Entry. The contents of other fields should be modified only as necessary to correct an error or to ensure proper processing of the Reinitiated Entry.

## Staff Training

Compliance with the *ACH Rules* should be a priority for every party involved in the origination of ACH Entries. Most ACH Origination Agreements contain language that allows the Originating Depository Financial Institution (ODFI) to pass on any

fines/penalties received because of an *ACH Rules* violation that is filed due to non-compliance on the part of the Originator or Third-Party Sender. To limit the likelihood of a fine or penalty, each Originator and Third-Party Sender should ensure that its staff receives regular training regarding its responsibilities for complying with the *ACH Rules*. Originators and Third-Party Senders that Reinitiate Return Entries should review *Article Two, Subsection 2.12.4, Reinitiation of Returned Entries*, as well as its procedures to ensure that batches containing the Reinitiated Entries meet the *ACH Rules* requirements that are discussed above.

Several requirements must be met to Reinitiate a Return Entry. Sometimes it can be overwhelming to look at all the requirements and know exactly what steps to take. If you find yourself in this situation, or if you're not quite sure if something should be treated as a Reinitiated Entry, contact your financial institution. 📞

## WEBPAGE continued from page 1

webpage, we caught up with Cash & Treasury Management Committee Member and EPCOR Board Member, Suzy Morris, APRP of Peoples National Bank in Mount Vernon, IL to discuss the new webpage and why it was created.

## What inspired the Corporate User Webpage?

"The Corporate User Webpage was inspired by the need to ensure corporate payment users had access to information to assist with their daily activities. As clients use tools differently, it is important to get the information in their hands, on their own terms."

## What do you hope users will get out of the webpage?

"I hope users will find resources to prevent risk or financial loss by sharing forward or

utilizing the tools provided on ACH, Wire and Check. Additionally, users may find other values from EPCOR through additional educational materials."

## What content will be available now and going forward?

"EPCOR will be sharing their *Payment Insider* newsletter, which has articles focused on relevant payment topics and updates occurring within various payment channels. Also, users will be able to access information on important updates to rules and regulations that could impact their daily activity."

## As a financial institution, what gaps in client education are you hoping to alleviate through the webpage?

"My organization, Peoples National Bank, is focused on educating and preparing our

clients to handle certain situations relating to transaction activity, including what to do when you get an ACH or Check Return. Having a site that has information on how to handle specific transactions will provide a direct resource without the financial institution having to translate or rebroadcast information which is available directly from EPCOR."

## How do you think your businesses can use the site's content to improve their payments processes/handling?

"I think our clients will use the content on the new webpage as needs occur when creating new payment transactions and whenever they are looking for a resource based on transaction type."

To check out the new Corporate User Webpage visit [epcor.org/corporateuser](https://epcor.org/corporateuser). 📞

# No Need to Panic: A Study in Third-Party Sender ACH Audits

by Nicole Payne, AAP, APRP, CPA, CRCM,  
CIA, Vice President, Advisory Services, EPCOR

One bright, sunny afternoon, Al strolled into the CPAs 'R Us mailroom at his usual time (right before the post-lunch sleepies kick in) to pick up the mail for the day. Shifting through the stack of envelopes, one caught his attention. It was from First Bank for You, the firm's financial institution. "Strange," he thought. "It's not time for the monthly statement, what could this letter be about? Maybe information about some new service they have rolled out..." As a Third-Party Sender, CPAs 'R Us occasionally received letters from the firm's financial institution with information about new cash management services. Al ripped open the envelope, ready to quickly scan and discard the letter. But he saw something that made him freeze. One little word: Audit.

Panic stricken, he scurried back to his desk with his mind racing. "What do they want? What kind of audit? How am I going to get through an audit...we're already busy enough!" he thought. Slinking into his desk chair, he took a deep breath to make himself calm down. Then he started from the top.

*"As an ACH Third-Party Sender, you are required to maintain compliance with the ACH Rules and complete an annual ACH*

*Rules Compliance Audit. Non-Compliance can lead to fines or even a suspension of your ability to originate entries through the ACH Network."*

"Fines!? Suspension?! I can't have that!" he thought to himself. "What do I have to do?! I'll do anything to avoid suspension!" He read on.

*"EPCOR is our go-to resource for guidance on the ACH Rules and other payment systems rules and regulations. We strongly encourage you to consider becoming an EPCOR member. They have a suite of services specifically designed to fit the unique needs of Third-Party Senders, including:*

## Third-Party ACH Audit Service

*A comprehensive review of your company's policies, procedures, and processes and whether they are compliant with the ACH Rules.*

## Third-Party ACH Risk Assessment

*A comprehensive evaluation of your payments operations against current regulatory guidance and industry best practices to identify potential risk issues and suggestions to mitigate them.*

## Third-Party ACH Consulting Services

*Intended to help you improve and strengthen your ACH Risk Management Program. This engagement addresses the entire range of processes from educating your sales staff to effectively managing your existing client relationships."*

"Ohhhh, whew!" Al thought, as he physically exerted the biggest sigh of relief. "At least there are some easy solutions! I've got this in the bag!" he thought. Al proceeded to check out EPCOR's website to see which of the recommended options he'd like to move forward with...the Third-Party ACH Audit Service did look pretty attractive to him since they already had so much on their plate. Al picked up the phone and dialed EPCOR. A pleasant voice answered the phone, "Hello, this is EPCOR, can I help you?" "Boy, can you ever!" Al responded.

If you find yourself in Al's shoes, holding a letter from your ODFI about ACH Audits, there's no need to panic! Skip right ahead to the solutions step and reach out to EPCOR to have your required ACH Compliance Audit conducted by a team of experts so you can get back to your day-to-day job. Contact us at [audit@epcor.org](mailto:audit@epcor.org) to book your service today! 📞



2020 was HEAVY! But... plutonium is back in stock and the payments industry has fired up the flux capacitor! Hop in the DeLorean with us for **EPCOR Payments Conference!**

Virtual • May 4 - 5  
Overland Park, KS • Oct. 25 - 27

REGISTER TODAY AT [EPCOR.ORG](https://epcor.org).

2021  
Nacha  
Operating Rules  
& Guidelines

The Guide to the Rules  
Governing the ACH Network  
Nacha

## ORDER YOUR DIGITAL COPY OF THE 2021 ACH RULES

Ensure compliance by making sure you are using the most current Rules available.

Access your digital copy on your desktop or via an app on your mobile device!



# Cashier's Checks: A Secure Alternative to Making a Big Cash Payment

by Marcy Cauthon, AAP, APRP, NCP,  
Director, On-Demand Education, EPCOR

Cashier's checks (issued by your financial institution) can offer more security than a personal or business check. Cashier's checks are generally meant to be used when you need to make or receive large payments securely. You may also choose to get a cashier's check in any situation where you need to make a payment, but you do not want the Payee to have your account information.

Cashier's checks can offer several benefits when making payments, but there are a few potential downsides. Here are a few things to keep in mind:

## Advantages of Cashier's Checks

- Funds are drawn against your financial institution's account and funds are guaranteed by the institution. The financial institution verifies that an account holder has enough cash or funds available in their account prior to issuing the cashier's check. Ensuring you have guaranteed funds to purchase the check can help you avoid having the check returned as insufficient funds and gives the party accepting the check peace of mind.
- Funds availability **may** be faster. Since cashier's checks are viewed as guaranteed funds, there may be a shorter hold period compared to personal or business checks.
- Security is increased. A cashier's check can reduce the potential for check fraud since only the person it is issued to can cash it. These types of checks typically feature enhanced security

provisions, such as watermarks, to prevent them from fraudulent duplication.

## Disadvantages of Cashier's Checks

- Cashier's checks are not foolproof. While they are more secure than other types of check payments, they are still a target to commit fraud.
- Financial institutions may charge a fee to purchase a cashier's check.
- Writing a personal or business check can get the funds to the party you are paying quicker as purchasing a cashier's check involves a trip to your financial institution. This could prove difficult if you need to make a payment outside of the institution's regular banking hours.

When purchasing a cashier's check at your financial institution, it is important to be specific about the payee and payment details. Once you request a cashier's check, the financial institution will draft the amount from your account and print it on the check. Getting the amount wrong could create problems if you need to ask the financial institution to reissue a new cashier's check.

One question often asked is, what happens if a cashier's check is destroyed, lost or stolen? If someone uses a cashier's check to pay you, it is important to keep careful track of it until you can deposit it at your financial institution. The same goes if you obtain a cashier's check from your financial institution to pay someone else. Replacing a destroyed, lost or stolen cashier's check isn't always an easy process. If you lose a cashier's check you

see **CHECK** on page 6

## Position Yourself Center Stage with Help from EPCOR

epcor®

Electronic Payments Core of Knowledge



AAP & APRP Prep Programs  
Kick Off Soon!

Watch our informational videos  
at [epcor.org](http://epcor.org) to learn more.

YOUR  
**GOALS**  
+  
OUR EXPERTS  
=  
**SUCCESS**

ACH • RDC • Wire

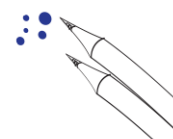
- Audits
- Risk Assessments
- Advisory Services

Visit [epcor.org](http://epcor.org) for  
more information

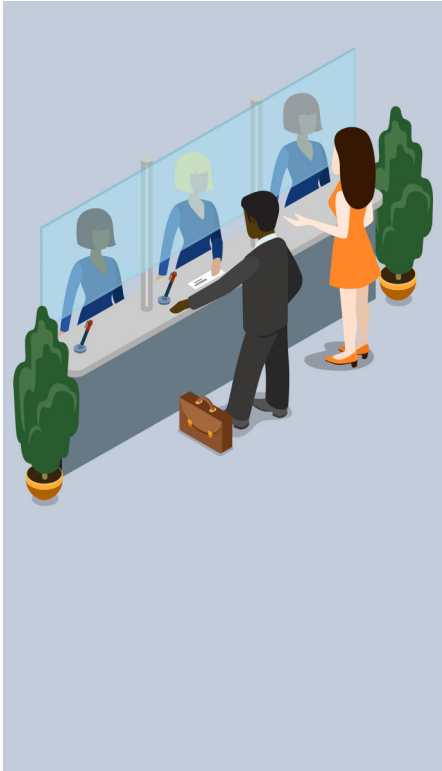


epcor®

Electronic Payments Core of Knowledge

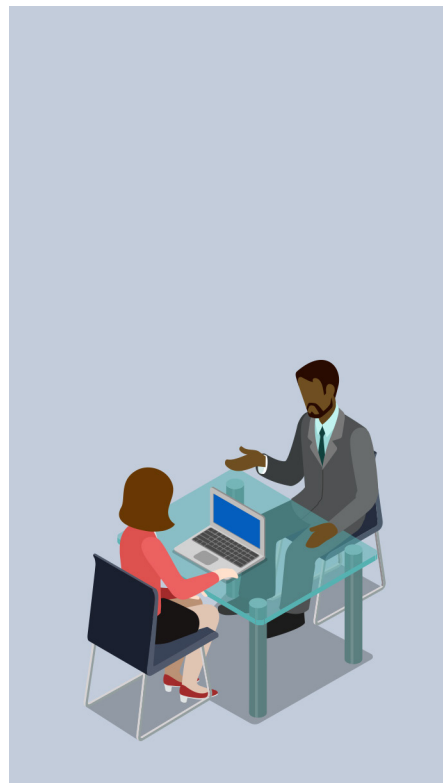


purchased from your financial institution, you may be required to obtain an indemnity bond for the amount of the check before they'll issue a new one. This essentially gives the institution some reassurance they will not have to cover the payment for both checks if the lost one is found and is presented for payment. While that sounds simple enough, it can take time to secure an indemnity bond through an insurance company.



Regulations state financial institutions must wait 90 days after the item was issued to give an account holder the option to complete a claim of destroyed, lost or stolen cashier's check and issue a replacement check. The 90 days is to give the original item enough time to clear the institution's account. This may be inconvenient if you still need to make a payment and do not have funds in your account to cover a new cashier's check. It is important to understand the claim form you sign has a clause that states you will be responsible to make the financial institution whole if the replacement check is presented as well as the original check.

If something happens to your cashier's check, you should understand a financial institution has limited options to help you resolve the matter. Financial institutions have a limited 24 hour window to return a check when it is presented to them for payment. And, the only acceptable reasons to return a cashier's check are if the check was altered, counterfeited, has a missing endorsement or the endorsement was forged. A cashier's check cannot be returned as insufficient funds or stop payment as the funds were guaranteed upfront. This gives your financial institution limited ability to help you in the event you misplace a cashier's check or it falls into the wrong hands.



So, next time you find yourself in need of purchasing a cashier's check, remember the funds are guaranteed as soon as the check is in your hands. If you need to send that check to a person or business through the mail, you may consider using registered mail next time to ensure it reaches its destination. Losing track of the check could be costly to you in the long run. 📌

Source: *Forbes*

# How the Pandemic is Accelerating the Shift from Cash to Digital Options

by *Nathan Lee, CNBC*

*This article originally appeared on December 3, 2020 on CNBC.com.*

The COVID-19 pandemic is expected to cause a drastic decline in cash usage due to the risk of contamination.

"Over the past six to eight months, we've seen the use of cash decline even further, and that's a trend I think that we're going to see continue," said Jodie Kelley, CEO of Electronic Transactions Association.

The unprecedented surge in the demand for contactless payment has also led to outstanding performances for major companies offering cashless methods, such as Apple, Square and PayPal. Dan Schulman, the CEO of PayPal, sees it as a sign that digital payments are shifting from "being a nice-to-have capability to a must-have essential service."

"When the pandemic hit, people really started paying attention to how literally they were spending money and people found that they didn't want to touch and exchange cash," Kelley continued.

There has already been a significant decrease in cash usage over the past few years. Nearly a third of U.S. adults said they typically make no purchase using cash during a week, according to a study by Pew Research Center.

Millennials are the ones leading the charge toward a cashless future. A report from

see **OPTIONS** on page 7

# Who is EPCOR? And, Could EPCOR Membership Benefit You?

EPCOR is a not-for-profit payments association that provides payments expertise through education, advice and member representation. While payments association membership may sound like something only financial institutions could benefit from, EPCOR offers an array of member benefits to support corporate payments users and individuals too.

EPCOR member Sandy Runyon, AAP, CCM, Corporate Treasury Consultant, has happily agreed to share her membership experience so you can decide if joining EPCOR is a good fit for your organization.

## How does EPCOR membership help you as a corporate payments user?

“EPCOR is a great source for obtaining knowledge. The payments industry has had so many changes, and with these changes come rules changes. EPCOR does a great job of communicating what is going on in the industry as well as providing educational opportunities.”

## What member benefits do you utilize the most?

“There are many benefits to enjoy that come along with being a member of EPCOR. I love the free *Quarterly Industry Update* webinars as well as *Payments Systems Update*. It's also so nice to be able to get a voice on the other end of the line when thinking through issues.”

## Why should other corporate payments users consider becoming an EPCOR member?

“Corporates need to stay up-to-date on rules and regulations. Without doing so, they could put themselves in a risky position. Being a member of EPCOR allows corporate payment users the resources and tools needed to stay current about what is happening in the payments industry and keep abreast of any required changes. EPCOR provides corporates the ability to have their voices heard and the opportunity to be included in shaping the future of the payments industry. Membership is reasonably priced and well worth the value.”

If you want to learn more about EPCOR membership, visit [epcor.org/join](https://epcor.org/join) or contact Member Support via phone (800.500.0100), email ([memserve@epcor.org](mailto:memserve@epcor.org)) or website live chat ([epcor.org](https://epcor.org)). 🗨️



OPTIONS continued from page 6

Experian in 2019 revealed that one in ten millennials use their digital wallet for every purchase. Pew Research also found that about 34% of adults under the age of 50 make no purchases in a typical week using cash.

Younger generations point to convenience as the main reason for switching from cash to contactless payments. “Not that I was using cash that much before, but I find that during the pandemic especially, I just don’t want to use cash as much because of the germ aspect,” explained Heima Sritharan, a cashless consumer.

Despite the rise in demand for contactless payments, many states and cities in the U.S. have passed laws banning cashless stores.

“There is a significant correlation between the use of cash, prepaid, debit, high-end credit and wealth, and there’s a huge correlation between wealth and race,” warned Aaron Klein, policy director at the Center of Regulations and Markets at the Brookings Institution. “Our payment system is geared toward helping the wealthy and charging the poor.”

Those within the industry maintain that the future of contactless payments remains promising. “I think we accelerated where we were going to be in three to five years. And in months, we jumped ahead, and I don’t think there’s any turning back from that,” said Schulman. 🗨️

Source: CNBC

## Can We Pat You on the Back for a Job Well Done?

Stellar Service?  
Innovative Products?  
Community Outreach?

Your efforts in the payments industry deserve to be recognized! Apply for an EPCOR Payment Systems Award at [epcor.org](https://epcor.org).



# Payment Fraud:

## What is it and How Can it Be Avoided?

*The following article originally appeared on BigCommerce.com.*

Payment fraud is any type of false or illegal transaction completed by a cybercriminal. The perpetrator deprives the victim of funds, personal property, interest or sensitive information via the Internet.

Payment fraud is characterized in three ways:

- Fraudulent or unauthorized transactions;
- Lost or stolen merchandise;
- False requests for a refund, return or bounced checks.

Businesses often rely on electronic transactions to charge clients for products and services. The increased volume of electronic transactions has also resulted in increased fraudulent activities.

### There are multiple methods of payment fraud:

- **Phishing:** Any emails or websites that require personal or private information such as credit card, bank account or login credentials are prone to phishing. If the source is trusted, such as a partner with a financial institution, the website is trustworthy. However, if the source is unfamiliar, it could indicate an attempt at stealing information.
- **Identity Theft:** Identity theft exists outside of the digital realm as well, but it's a common type of fraud online. A cybercriminal who steals personal information and uses it under false pretense is engaging in identity theft. Hackers penetrate firewalls through old security systems or by hijacking login credentials via public Wi-Fi.

- **Pagejacking:** Hackers can reroute traffic from your website by hijacking part of it and directing visitors to a different website. The unwanted site may contain potentially malicious material that hackers use to infiltrate a network security system. Business owners must be aware of any suspicious online activity in this capacity.
- **Advanced Fee and Wire Transfer Scams:** Hackers target credit card users and businesses by asking for money in advance in return for a credit card or money at a later date.
- **Merchant Identity Fraud:** This method involves criminals setting up a merchant account on behalf of a seemingly legitimate business and charging stolen credit cards. The hackers then vanish before the cardholders discover the fraudulent payments and reverse the transactions. When this happens, the payment facilitator is liable for the loss and any additional fees associated with credit card chargebacks.

### How does fraud happen?

Fraudsters have become savvy at illegally obtaining information. Hackers often pose as a legitimate representative and contact credit card owners asking for sensitive information, then use the following means of interaction to steal personal data:

- Email
- Texting malware to smartphones
- Instant messaging
- Rerouting traffic to fraudulent websites
- Phone calls
- Online auctions

Cyberthieves also work in teams to penetrate network security systems by looking for glitches or patches that haven't been updated in a while. These gaps give hackers access around a firewall and make it easy to illegally obtain sensitive information.

### How can ecommerce businesses mitigate fraud?

While it's challenging to eliminate the threat of fraud, you can help protect against it by continually updating your network security systems. Firewalls and antivirus software are designed to act as a shield against hackers' attempts to penetrate a secure network. Constantly updating software helps ensure that your sensitive business information is safe.

There are several other ways to protect your business against fraudulent payments:

- Maintain awareness of the latest fraud trends
- Partner with a verified payment processor
- Encrypt transactions and emails containing confidential information
- Ensure that tokens and login credentials are regularly changed
- Establish a policy regarding access to confidential information
- Constantly run security checks with antivirus software
- Require clients to log in to an individual account prior to making a purchase

Payment fraud can hurt both you and your clients. By aggressively protecting your organization against fraud, you can improve your reputation and your bottom line. 🟢

*Source: BigCommerce.com.*





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](http://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.

© 2021, EPCOR. All rights reserved.

[www.epcor.org](http://www.epcor.org)

3100 Broadway Blvd., Ste. 555, Kansas City, MO 64111

800.500.0100 | 816.474.5630 | fax: 816.471.7665