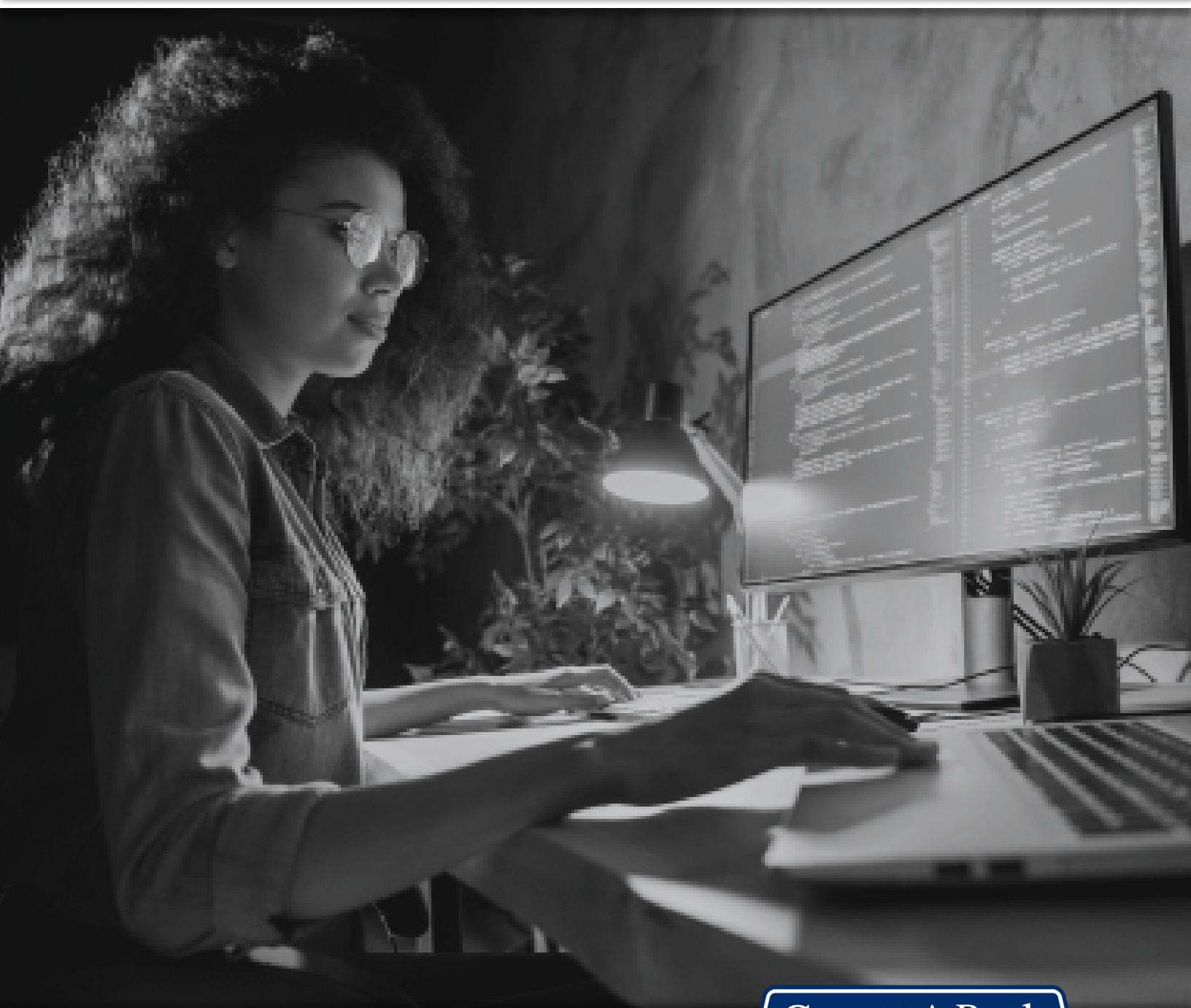


ACH Payment Scams Threatening Distributors



Comerica Bank

®

comerica.com



Contents

Introduction	01
Which organizations are most likely to be targets of payments fraud?	02
Who is at risk for ACH payment scams?	03
What is involved in ACH fraud?	04
How can my business prevent ACH payment scams?	05



Introduction

Scams and fraudsters are an unfortunate fact of life for businesses across the modern economy.

While many types of companies are at risk for fraud, distributors such as merchant wholesalers often deal with a high volume of suppliers, customers and merchandise. Established distributors also have yearly

sales volumes in the tens or hundreds of millions of dollars. These circumstances can make merchant wholesalers prime targets for criminals attempting to commit a variety of fraud.

Automated Clearing House (ACH) payments are a vital tool for distributors to compensate suppliers and receive funds

from customers. With so much money flowing into and out of merchant wholesalers through ACH payments, the system can be a common target of fraudsters. Learning more about ACH payments, related fraud risks and strategies your business can use to mitigate risk means building a more secure foundation for your operations.



Which organizations are most likely to be targets of payments fraud?

All types of businesses are at risk for general payments fraud. The 2020 Payments Fraud and Control Survey, published by the Association for Financial Professionals® (AFP), found 81% of respondents reported facing an attempted or successful payments fraud attack in 2019. Additionally, payments fraud has increased

somewhat in recent years, based on the findings of the AFP. A large majority of businesses can expect to experience a similar issue as time goes on.

Fraudsters may attempt to target both large and small organizations. A lack of strong or established security measures

could lead criminals to focus on smaller businesses. However, the substantial assets of many large enterprises — and the fact that a minority may not have sophisticated fraud detection and prevention strategies and systems in place — make them attractive targets to some scammers.



Who is at risk for ACH payment scams?

Any company that utilizes ACH payments could be at risk for ACH fraud. The motivations and goals of scammers can differ greatly from one individual or group to the next. The safest assumption to make is that your company can experience an attempt at payment fraud.

ACH payments are a common transaction type in the business-to-business realm. The National Automated Clearing House Association® predicted that, in

2020, ACH payments will surpass checks as the most popular form of B2B payment. Because of their long history of widespread use and increasing popularity, companies that regularly utilize ACH payments may find themselves targeted by fraudsters.

While every business is different, many merchant wholesalers regularly turn to ACH payments. There are a number of advantages, including avoiding

the need to physically handle and secure currency or checks, fast processing times and the automated nature of the ACH system. It's important to note that ACH payment scams by themselves are not a reason to move away from this type of transaction. With proper security measures in place, your business can continue to use ACH payments confidently and securely.



What is involved in ACH fraud?

ACH transactions require an authorized user of an account to authorize a payment. Fraud occurs when an unauthorized individual gathers the necessary information to impersonate an authorized user and send a payment. The stolen money could go into an account associated with the person or group taking the criminal action or to pay for the purchase of goods or services.


ACH payment scams can be a simple or complex practice, depending on the resources of the involved criminals. A defining component of ACH fraud is that only two pieces of information are

needed to engage in this illegal practice. A checking account and bank routing number, which are easily found on checks issued by a business, provide enough detail for a properly equipped scammer to start the process.

This information may be accessed by any number of means. Criminals may gain access to a canceled or current check written by the target company. In cases where fraudsters can't find, steal or otherwise obtain a check, they may turn to other strategies. Scammers could attempt to use phishing, impersonating a financial institution, business partner or

other trusted organization or individual via email. They may also rely on similar tactics on the phone or through other methods of communication to induce an employee to share the necessary information. They might also attempt to infect an organization's computer network with keylogger software, which can provide the information.

No matter how the sensitive data is secured, the end result is the same: The fraudsters will transfer money from a business into another account.



How can my business prevent ACH payment scams?

While ACH payment scams can be very damaging, there are many common security measures businesses can take to minimize the possibility of this crime affecting them.

Training employees to recognize signs of phishing and similar schemes used to extract sensitive information can lower the odds of those efforts being successful. Implementing anti-malware software can identify and eliminate malicious programs, including

keyloggers. Regularly checking account balances and establishing fraud alerts through online banking makes it easier to spot fraudulent transactions. This safeguard will also help you notify your financial institution about ACH payment scams in a timely manner.

Banks **may also offer tools** that help secure accounts used to process ACH payments. Comerica ACH Positive Pay™, for example, allows users to **authorize or deny any activity** before it posts. Other

tools sometimes seen for fighting fraud include debit blocks on accounts not intended for ACH withdrawals and filters that limit ACH debits to specific amounts or organizations authorized to do so.

Working with a knowledgeable and trustworthy financial institution that understands the importance of secure ACH transactions is a critical part of defending against fraud. Get in touch with the team at Comerica Bank today to learn more.



Comerica Bank

Sources:

<https://www.prnewswire.com/news-releases/survey-business-email-compromise-most-common-cause-of-fraud-attempts-301036189.html>

<http://go.nacha.org/crfsurveyresources>

This information is provided for general awareness purposes only and is not intended to be relied upon as legal or compliance advice for your business.

This article is provided for informational purposes only. While the information contained within has been compiled from source[s] which are believed to be reliable and accurate, Comerica Bank does not guarantee its accuracy. Consequently, it should not be considered a comprehensive statement on any matter nor be relied upon as such.

Comerica Bank
Member FDIC
Equal Opportunity Lender
© 2020 Comerica Incorporated