Business-to-Business Payment Fraud

PRACTICAL INSIGHTS FROM HUNTINGTON

Payment fraud in business-to-business (B2B) financial transactions is a problem that's not going away. Paper check fraud is still the most prevalent form, and technology is providing criminals new ways to effectively scam businesses.

With companies facing the potential for payment fraud on multiple fronts and an increasing number of attacks, CFOs and Treasurers need to understand the risks and take action to manage, control and mitigate those risks.

In this report, we'll share the basics of payment fraud and offer strategies you can use to help protect your company against it—a critical move for business leaders who want to help ensure the continued vitality and longevity of their companies.

82%

of companies surveyed were targets of payment fraud in 2018—the highest level ever reported†.

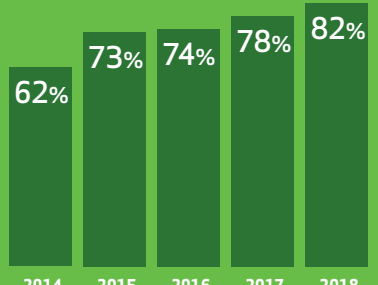
WHO'S AT RISK?

No organization is immune. Of the 617 firms responding to the 2019 Association for Financial Professionals (AFP) *Payments Fraud and Control Survey*, 82% report their organizations were targets of payment fraud in 2018—the highest level ever reported in the 15 years of the survey†.

Furthermore, 34% of respondents reported an increased number of payment fraud attacks in 2018†. Larger organizations with more payment accounts were the most likely to see an increase in attacks.

These numbers suggest that criminals are succeeding in their attempts to swindle companies and will continue to target more organizations over time.

Percentage of Organizations That Experienced Attempted and/or Actual Payments Fraud†



"Payments fraud is a persistent problem that is only getting worse despite repeated warnings and educational outreach," said Jim Kaitz, AFP president and CEO, in a statement. "Treasury and finance professionals need to learn the latest scams and educate themselves—and perhaps more importantly—their work colleagues on how to prevent them‡."

HOW DOES IT HAPPEN?

Payment fraud ranges from age-old tactics to new, technology-driven methods. The most common types of fraud reported in the AFP survey are as follows:

Check Fraud

Check fraud continues to be the most common type of payment fraud, as paper checks remain a commonly used payment method by businesses†. Fraudsters can acquire unsecured check stock directly from the business or intercept mail to get a check that they will chemically wash to alter payment information.

Wire Transfer Fraud

This type of fraud has grown to become the second-most reported type of payment fraud—increasing

800% since 2011. The dramatic increase in wire transfer fraud is commonly associated with an increase in Business Email Compromise (BEC) tactics[†]. (We'll detail more about BEC later in this section.)

800%

Wire transfer fraud has grown 800% since 2011, more than all other types of payment fraud[†].

ACH Fraud

Though ACH is considered more secure than checks, a 17.86% increase in reported ACH debit fraud from 2017 to 2018[†] could indicate that criminals are getting savvier at bypassing current security measures.

Corporate Credit Card Fraud

Currently the fourth-most common type of payment fraud[†], incidents of credit card fraud tend to have more upward and downward swings from year to year that seem to coincide with large data breaches at retailers where card data was stolen.

"Businesses may not notice fraud attempts right away because criminals might test a small amount first," said Ashley Sutor, senior vice president, enterprise payments and fintech program manager at Huntington. "Once they have routing and account numbers, they attempt a $5 or $10 transaction. If that's successful, they continue to access the account for more money. Businesses need a full account reconciliation to guard against fraud[§]."

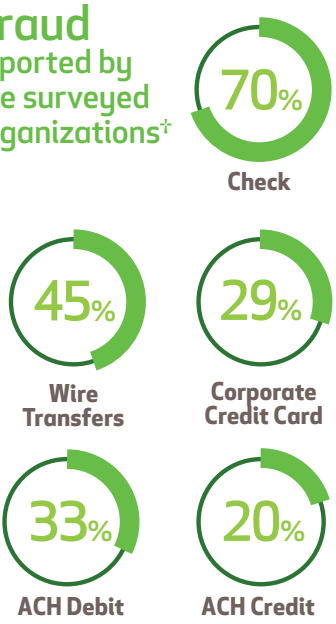
Business Email Compromise

Business Email Compromise (BEC) is a tactic that fraudsters are increasingly using to trick unsuspecting company personnel into making an unauthorized transfer of funds. Commonly, the criminals spoof the email account of an established vendor and request the company wire all future invoice payments to an alternate, fraudulent account. Or they hack an executive's internal email account and send an urgent request for a funds transfer directed to the criminals' account[†].

"BEC scams have evolved beyond the fraudulent transfer of funds," says Jessica Greene, vice president, treasury management fraud at Huntington. "During the last tax season, criminals targeted human resource departments posing as company executives requesting employee W2 information via email. This information was then used in a variety of identity theft scams[#]."

Percentage of Attempted/Actual Fraud

reported by the surveyed organizations[†]



Business Email Compromise Fraud in the U.S.

In 2018, the FBI Internet Crime Complaint Center received reports from more than 20,000 victims of BEC fraud in the United States claiming nearly $1.3 billion in exposed dollar loss[¶].

20,373 victims

$1.29 billion in exposed loss

Huntington®

Tips to Help Prevent Business Email Compromise Payment Fraud

- Be suspicious of requests for secrecy or to take action quickly.
- Don't rely on email when requests are made to change payment instructions. Verify using a known phone number.
- Beware. Criminals attempt to make emails look legitimate by using the name and logo of a real company.
- Look for poorly worded messages and grammatical errors.
- Remember that government agencies will never request a wire transfer.
- Watch for phrases "code to admin expenses" or "urgent wire transfer" found in many fraudulent communications.
- Create an environment where staff members feel comfortable voicing concerns when they think something is amiss.
- Implement a dual approval process to verify whether the transfer should occur.

Account takeover is a growing concern for businesses as well. In account takeover, a fraudster gains control of a customer's account and places an order shipped to him instead of the true account holder. Since only the shipping address changed on the order, merchants rarely identify it as fraudulent.

According to data from Forter's 2019 Fraud Attack Index, Account Takeover (ATO) has remained high, increasing by 45% by the end of 2018 compared to the beginning of 2017[¥].

WHY DOES IT MATTER?

The potential financial loss from an attempted or actual payment fraud can create a serious hardship for a company.

Thirty-one percent of businesses that responded to the AFP survey as having experienced payment fraud reported potential losses of $250,000 or more. And a staggering 12% of those expect potential losses of $2 million or more[†].

"It's not just about the stolen money," said Will Carlin, D & O and cyber product manager for Huntington Insurance. "Many businesses don't even consider that the cost also includes lost productivity from staff shifting focus to investigating the incident and any technology investments or process remediation that is required to prevent future fraud[¥]."

31%

of surveyed businesses that experienced payment fraud reported $250,000 or more in potential loss[†].

Plus, fraud can expose y our confidential business and personnel information, which can impact your organization's reputation and put your valued employees at risk.

"Most companies focus on the immediate monetary loss. But there's a reputational risk to payment fraud," said Sutor. "If other companies don't believe payments are safe, they may shy away from doing business with you[§]."

Bottom line: Not having protection against fraud leaves an organization exposed to unnecessary risk and expense.

WHAT CAN YOU DO?

Companies cannot be complacent in their efforts to manage and mitigate payment fraud. The most important step is to create a plan.

"Businesses need a fraud plan in place to know exactly what steps to take when an incident happens. For example, do you know who to call first if you experience fraud? You should," said Sutor. "We'll help you figure it out[§]."

Your bank can be a great resource for advice and assistance in establishing your payment fraud plan.

"A knowledgeable institution, like Huntington, can help a business establish a proactive defense," said Greene. "Over the years, we have helped many clients deal with payment fraud attacks. Using that experience, we have developed products and services that can help organizations of all kinds minimize their exposure[#]."

PERSPECTIVE

"Fraud mitigation should be part of your overall payment strategy, and your financial institution should guide you when planning for this scenario and when proposing other ways to help protect your company.[≠]"

— Adriana Hastings, senior vice president, treasury management director for Huntington

For example, Huntington offers a **Business Security Suite of Treasury Management products** designed to help guard against both paper and electronic payments fraud.

At the heart of the Business Security Suite is Check Positive Pay and ACH Positive Pay. Check Positive Pay is a daily verification process to detect fraudulent, altered or counterfeit checks by matching all issued checks to a check-issue file you provide. If the dollar amount, check number and account don't match, the check is flagged. ACH Positive Pay helps you control your ACH transactions using filters and blocks.

Check Block is another product in the Business Security Suite. It designates your business checking account to make only electronic transactions. All paper-based activity is automatically rejected to eliminate altered, stolen or forged check fraud. Wire Block is an electronic fraud mitigation solution that helps reduce the risk of wire fraud by blocking wire debits from coming out of your business account.

Huntington also provides **Cyber Liability Insurance** through Huntington Insurance[Ł]. By offering insurance coverage in addition to standard financial services, Huntington offers a more comprehensive and convenient way to help businesses protect themselves against the negative impacts of payment fraud[Ł].

Customized cybercrime insurance coverage can include any or all of the following:

- Breach Response/Crisis Management
- Cyberextortion
- Business Interruption Extra Expense Loss
- Data Restoration Coverage
- Network Security Liability
- Privacy Liability
- Regulatory Coverage
- Website Media/Multimedia Coverage
- Professional Liability

For businesses that need to upgrade technology or replace aging IT infrastructure as part of their payment fraud mitigation plan, Huntington has a variety of financing options to assist with updates[Ω].

Ask your banker to help review the risk management plan for your business. It's a great way to help identify potential gaps and learn about what products and services will make the greatest impact on your ability to defend against payment fraud.

About Huntington

Huntington Bancshares Incorporated is a regional bank holding company headquartered in Columbus, Ohio, with $108 billion of assets and a network of 868 full-service branches, including 12 Private Client Group offices, and 1,687 ATMs across seven Midwestern states. Founded in 1866, The Huntington National Bank and its affiliates provide consumer, small business, commercial, treasury management, wealth management, brokerage, trust, and insurance services. Huntington also provides vehicle finance, equipment finance, national settlement, and capital market services that extend beyond its core states.

Visit huntington.com for more information.

---

† *2019 Association for Financial Professionals (AFP) Payments Fraud and Control Survey Report. Association for Financial Professionals. April 2019.*

‡ *"Corporate Payments Fraud Jumps Despite Stronger Internal Controls." PYMNTS.com. April 10, 2019*

§ *Ashley Sutor interview. September 26, 2019.*

¶ *2018 Internet Crime Report. Federal Bureau of Investigation. April 22, 2019.*

Jessica Greene interview. September 26, 2019.

¥ *2019 Fraud Attack Index. Forter. March 12, 2019.*

¥ *Will Carlin interview. October 4, 2019*

≠ *Adriana Hastings interview. October 11, 2019*
