Huntington®

Practical Insights:
Business-to-Business Payment Fraud
IS YOUR COMPANY AT RISK?

Practical Insights: Business-to-Business Payment Fraud

Payment fraud in business-to-business (B2B) financial transactions is a problem that's not going away. Paper check fraud has shown an uptick, 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 guide, 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.

HIGHLIGHTS:

74% of companies surveyed were victims of payment fraud in 2016—the highest level ever reported.*

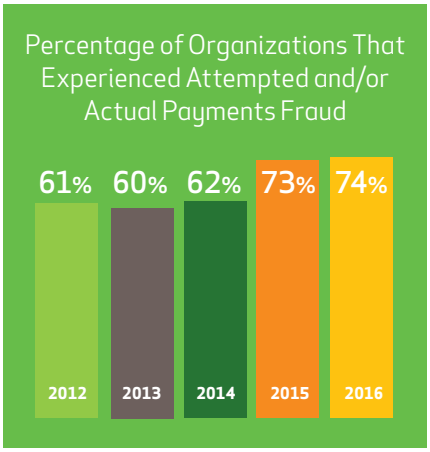
Check fraud remains the most common type of payment fraud. However, wire transfer fraud has grown 40% since 2011, more than all other types of payment fraud.*

29% of businesses that experienced payment fraud reported potential losses of $250,000 or more. And a staggering 8% project more than $2 million in potential losses.*

WHO'S AT RISK?

No organization is immune.

Of the 547 firms responding to the 2017 Association for Financial Professionals (AFP) *Payments Fraud and Control Survey*, **74% report their organizations were victims of payment fraud in 2016**—the highest level ever reported in the 13 years of the survey.*



*Source: Association for Financial Professionals**

Furthermore, 36% of respondents reported an increased number of payment fraud attacks in 2016.* 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.

"We saw even more payments fraud this year than last year, and that by itself, to me, is a surprise," Magnus Carlsson, AFP Manager, Treasury & Payments, told payment industry news site PYMNTS.com. "The huge increase last year was so big that I didn't think it would continue this way."†

Huntington®

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 40% 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.)

Corporate Credit Card Fraud

Currently the third-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.

ACH Fraud

Though ACH is considered more secure than checks, a 5% increase in reported ACH debit fraud from 2015 to 2016 could indicate that criminals are getting savvier at bypassing current security measures.

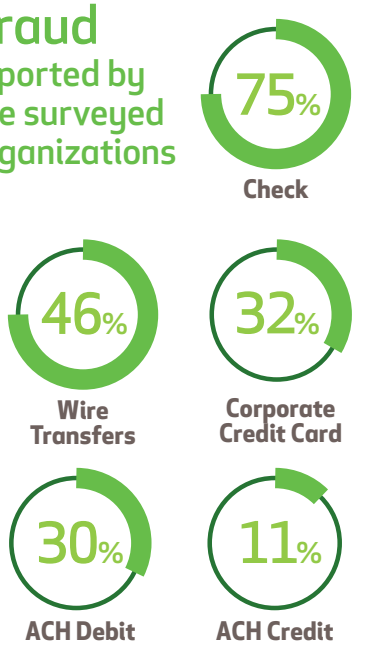
"Businesses may not notice fraud attempts right away because criminals might test a small amount first," said Ashley Sutor, Senior Vice President, Treasury Management Strategy & Execution at Huntington. "Once they have routing and account numbers, they attempt a $5 or $10 transaction. If that's successful, 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.

Percentage of Attempted/Actual Fraud

reported by the surveyed organizations



*Source: Association for Financial Professionals**

Business Email Compromise Fraud in the U.S.

Between October 2013 and December 2016, the FBI Internet Crime Complaint Center received reports from more than 22,000 victims of BEC fraud in the United States claiming nearly $1.6 billion in exposed dollar loss.

22,000+ victims

$1.59 billion in exposed loss

*Source: FBI Internet Crime Complaint Center**

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.

"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."

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 the October 2017 Global Fraud Index, **account takeovers have increased 45% in the second quarter of 2017**, exposing merchants to $3.3 billion in loss in just those few months alone. [§]

WHY DOES IT MATTER?

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

Twenty-nine 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 8% of those expect potential losses to exceed $2 million.*

29%
of businesses
that experienced payment fraud reported
$250,000
or more
in potential loss

"It's not just about the stolen money," said Thom Jenkins, Senior Vice President, Energy & Technical Risk 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."

Plus, fraud can expose your 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.

PERSPECTIVE

"Fraud mitigation should be viewed in conjunction with an overall business continuity strategy, and your financial institution should be helping your business operate and be successful."

— Steve Rhodes, Executive Vice President, Treasury Management Director

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."

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 lets 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 fraud from altered, stolen or forged checks.

Huntington also provides **Cyber Liability Insurance** through Huntington Insurance.‖ 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.

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

- Breach Response/Crisis Management
- Cyberextortion or Loss
- 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 and are vulnerable to attack, Huntington has a variety of financing options# to make the updates easy.

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

Talk to Huntington about cybersecurity tools, best practices, and resources you may want to consider as you develop an approach to protecting your organization.

huntington.com/Banking-That-Cares

About Huntington

Huntington Bancshares Incorporated is a regional bank holding company headquartered in Columbus, Ohio, with $104 billion of assets and a network of 966 branches and 1,848 ATMs across eight 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 auto dealer, equipment finance, national settlement and capital market services that extend beyond its core states. Visit huntington.com for more information.

** Association for Financial Professionals. 2017 Payments Fraud and Control Survey. March 2017.*

† PYMNTS.com. Breaking Down the Data Behind Record Levels of B2B Payments Fraud. 14 April 2017.

‡ Federal Bureau of Investigation. Business E-mail Compromise/E-mail Account Compromise: The $5 Billion Scam. 4 May 2017.

§ PYMNTS.com. Global Fraud Index–October 2017. October 2017.
