



ASSOCIATION FOR
FINANCIAL
PROFESSIONALS

AFP Payments Guide

Not Going Anywhere: Why Checks Still Matter

Underwritten by





Companies across all sectors continue to face growing challenges in cybersecurity and payments fraud when managing their working capital. It's important that corporate treasurers and CFOs have the latest research and information as they navigate the rapidly evolving payments landscape. That is why MUFG Union Bank, N.A., is pleased to sponsor our fourth *AFP Payments Guide: Not Going Anywhere: Why Checks Still Matter*¹.

Despite prevention education and advances in fraud detection, incidents of fraud remain high. According to the *2017 AFP Payments Fraud and Control Survey*², 74 percent of finance professionals report that their organizations were targets of payments fraud in 2016, and of those 75 percent were victims of check fraud.

This current business environment underscores how critical the data, examples, and prevention strategies in this *AFP Payments Guide* are for financial professionals to help recognize and combat fraud. While payment breaches may not be completely preventable, services available from banks, together with the actionable information in this guide, can help to reduce occurrences.

We support the AFP in its commitment to education and raising awareness of cyber threats and potential fraud risks. We plan to share this guide with our clients and discuss strategies to help mitigate risks to their operations.

Best regards,

A handwritten signature in black ink that reads "Ranjana Clark".

Ranjana B. Clark
Head of Transaction Banking Americas and Bay Area President
MUFG Union Bank, N.A.

¹ The Research Department of the Association for Financial Professionals®, which designed and conducted the research and wrote the report, is solely responsible for its content.

² Article from AFP, published March 2017.

©2017 Mitsubishi UFJ Financial Group, Inc. All rights reserved. The MUFG logo and name is a service mark of Mitsubishi UFJ Financial Group, Inc., and is used by MUFG Union Bank, N.A., with permission; Union Bank is a registered trademark and brand name of MUFG Union Bank, N.A., Member FDIC.

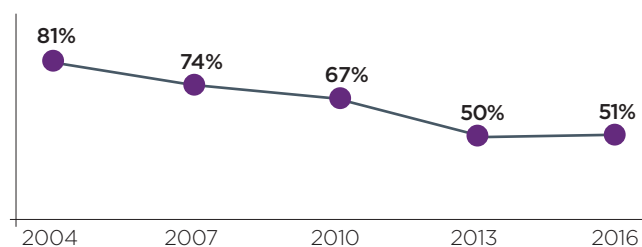
Paying by check is antiquated, expensive and easily susceptible to fraud. It's also essential if you're a treasurer for a U.S. corporation. In the United States, check use for business-to-business (B2B) transactions remains at roughly 50 percent despite a multitude of recent advances in payments technology. Simply put, checks aren't going away any time soon in the United States.

In this latest AFP Payments Guide, sponsored by MUFG Union Bank, we will review precisely why so many corporates still use checks for B2B payments, why checks are the payment method most susceptible to fraud, and what treasury professionals can do to protect themselves when paying by check.

Why 1 Percent Matters

When AFP published the **2016 AFP Electronic Payments Survey**, one particular data point stuck out. B2B payments by check actually increased by 1 percentage point from 2013 to 2016. "While 1 percentage point might not sound like a lot, you have to understand that we've observed check use to be declining since 2004, back when it was at 81 percent," wrote Magnus Carlsson, AFP's manager of treasury and payments, in a **blog post** late last year. He went on to note that the survey runs every three years and with each increment, check use has decreased substantially—until now.

Percentage of Organization's B2B Payments Made by Checks
(Percentage of B2B Payments Made by Organizations)



Source: 2016 AFP Electronics Payment Survey

The small increase can be attributed to larger organizations using checks more often. The survey found that check usage at businesses with annual revenues of \$1 billion or more went from 40 percent to 45 percent. Surprisingly, smaller organizations—which are typically known for clinging to checks—actually reduced check usage by 3 percentage points over the same time period.

But as Carlsson explained, larger organizations may be victims of their own success. The bigger your company is and the more departments it has, the harder it can be to change payment processes. Treasury departments usually need to receive approvals from multiple parties before they can make a sweeping change, and eliminating checks certainly would qualify.

"Over the last year, we've seen some of the companies ordering more checks. And what we're told is that they are so afraid of the cyberthreats that they would rather issue a check."

There is another factor, however, that is even more alarming: Some corporates keep checks because fraud schemes focused on other payments are skyrocketing.

Greg Litster, president of high-security check provider SAFEChecks, said he has corporate customers who have diminished check use substantially in favor of e-payments—but then moved back to checks. "Over the last year, we've seen some of the companies ordering more checks," he said. "And what we're told is that they are so afraid of the cyberthreats that they would rather issue a check."

Despite the well-founded fear of cyberfraud, check fraud remains the payment method fraudsters target the most. According to the **2017 AFP Payments Fraud and Control Survey**, 75 percent of organizations experienced check fraud in 2016, an increase from 71 percent in 2015. AFP had been observing a declining trend in check fraud since 2010—but that all changed last year.

Why Checks?

Fully 51 percent of organizations' B2B payments are made by check, according to the 2016 AFP Electronic Payments Survey. Many corporates typically use checks for B2B payments to smaller suppliers who either aren't equipped to go electronic or don't want to deal with the hassle of converting. For example, Tom Wolfe, CTP, senior director of global treasury for Marriott Vacations Worldwide Corporation, noted that 27 percent of the payments his company makes to suppliers are by check.

Checks also remain heavily in use for business-to-consumer (B2C) payments. Eric Matheny, vice president of corporate finance and treasury for Allianz Global Corporate

and Specialty, said that about 68 percent of the claims payments Allianz makes to clients are by check.

One key reason why checks won't go away for many corporates? Their legacy payments systems. Many of these systems, even at large companies, are so old that they are only set up to send paper checks. "We are going through that process now; we're putting in some new technology to replace these old legacy systems, to encourage more electronic payments and collections," Matheny said.

Additionally, U.S. corporates employ a concept called dual payee, in which an organization may need to make one payment to two separate entities. "Let's say you make a payment to the insured and their lawyer—you can't do that with a wire, so you have to use a check," Matheny said. "That's one reason why checks are so prevalent with insurance companies."

Bill Booth, former executive vice president of treasury management for a major bank, continues to see corporates moving to electronic payments (including purchasing cards) wherever they can, particularly for B2B. "They're trying to identify ways to eliminate checks in the first place," he said. "That might be segmentation of certain payees; they can't completely eliminate checks, but they are taking steps to try and electronify routine payments to known vendors."

By and large, however, the biggest hurdle is a cultural one. Americans simply are comfortable with checks despite high fraud rates. "I think there is a misconception that receiving a paper check is safer than providing banking details for an electronic payment," Matheny said. "They're thinking, 'If I give my bank information to this company and they get breached, then they could get my information. So just send me a check. Then all they have is my address and I feel more secure.' So a lot of this might be customer driven. That's why, in my mind, nothing is going to happen until there is a country mandate that there will be no more paper checks."

High Costs

Checks also are more expensive than electronic payments—16 times more than ACH to process, according to Wolfe—due multiple factors including issuing checks, paying checks, payee verification, postage, image capture and storage, recon service, and more.

Fraud prevention measures are perhaps the most significant expense. Wolfe noted that they can vary significantly by bank. "But you don't know what the consequence is if you don't have those controls in place," Wolfe said. "Maybe you lose \$1,000.

Maybe you lose \$50,000. You have to look at the cost-benefit, and there's really no way to calculate that in this day and age."

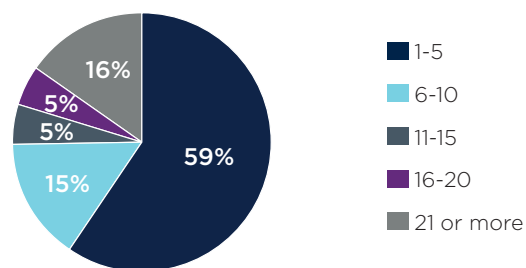
One way that corporates can reduce check expenses is by outsourcing printing and mailing to the bank. "We send a file to our banking partner and they print the check and mail it to the payee," said Matheny. "This reduces your cost dramatically, versus producing a check in-house, which can be \$7 to \$8 per check. It also automatically issues the check for us at the bank for positive pay purposes, and it eliminates any in-house handling time of the check."

However, corporates that outsource check disbursements should read the contract with their provider carefully to determine which party has the liability for check fraud losses, Litster noted. Though the process may be outsourced, check fraud risk might remain with them. "If the contract is silent, the company very likely has the liability," he said.

Educating check users also helps reduce costs. The treasury department at Allianz has had frequent discussions with the claims department about how it can propose electronic payment at the time of a claim settlement. "Our customer goal is to make timely and accurate payments, and so a move away from paper checks is fully consistent with this goal, and yet will probably require more education for everyone on the benefits of electronic payments versus a paper check," Matheny said.

Number of Times Organization Experienced Attempted and/or Actual Check Fraud in 2016

(Percentage Distribution of Organizations that Experienced At Least One Attempt of Check Fraud)



Source: 2017 AFP Payments Fraud and Control Survey

Check Fraud

The 2017 AFP Payments Fraud and Control Survey found that 59 percent of organizations experienced between one to five attempts at check fraud in 2016. Fully 15 percent were subject to between six and 10 incidents, while 16 percent were exposed 21 or more times. Organizations with revenues

exceeding \$1 billion were the most likely victims of fraud throughout the year—31 percent reported experiencing more than 15 instances of check fraud in 2016.

Perhaps no one knows more about check fraud than Frank Abagnale, the reformed check forger whose life story was the basis of the popular Leonardo DiCaprio film, “Catch Me if You Can”. Abagnale, who now works as a security consultant for the federal government and Fortune 100 companies, said he thought he would be done with check fraud by now, but it simply won’t go away.

Abagnale noted that a skilled fraudster can create a check that looks completely legitimate in just 15 minutes. However, the most important part of the process involves social engineering, i.e., human error.

Using an airline as an example, Abagnale said a forger would first call the main number and ask to speak to someone in accounts receivable. “Accounts receivable answers, the forger says, ‘We’re getting ready to pay this invoice you sent us but we’d prefer to wire you the funds. We just need your wiring instructions,’” he said. So the AR employee gives the bank name and the account number. After that, the forger calls the airline’s corporate communications department and requests the company’s annual report. Page three of that report contains the signatures of the chairman of the board, the CEO, the CFO, the treasurer and the controller. From there, the forger has everything they need to create a fake check. “What I did 50 years ago is 4,000 times easier today,” he said.

“Check fraud hits companies that are small and unsophisticated, and ones that are large and—theoretically—sophisticated.”

While check fraud is the most prevalent fraud method, it’s far from the most successful. Fully 55 percent of organizations experienced check fraud in 2016, according to AFP’s fraud survey, but only 10 percent actually experienced a financial loss.

Still, the threat is not to be taken lightly. Booth has observed check fraud impacting companies of all sizes. “My sense is that it’s trending down a bit, but check fraud hits companies that are small and unsophisticated, and ones that are large and—theoretically—sophisticated,” he said.

Positive Pay and Payee Positive Pay

According to the 2017 AFP Payments Fraud and Control Survey, positive pay is the method most used by organizations to mitigate check fraud. Fully 74 percent of organizations and 82 percent of organizations with annual revenues over \$1 billion use the protection. Some banks are seeing even higher adoption. “Nearly 90 percent of our ARP accounts have some form of positive pay service,” said Jeffrey Felser, senior vice president of commercial payments within treasury management at PNC Bank, N.A. “This percentage and the number of accounts on positive pay services continues to grow.”

Positive pay matches a list of issued checks from an organization with those presented for payment. If the bank finds any discrepancies, it sends them back to the issuer. “Positive pay, in my opinion, is probably the best technology in the world to prevent forgery,” Abagnale said. “There’s no excuse today not to have a secure check.”

But standard positive pay only matches the amount and the check number. For corporate treasury departments that make a lot of payments by check, it is absolutely critical to use payee positive pay, also known as payee name authentication (PNA). This technique verifies the payee name, amount and check number. Allianz uses PNA on all of its disbursement bank accounts. Matheny added that this has helped immensely, given a recent influx of fraud attempts by criminals changing the payee name.

While some changes to the payee information are obvious—such as a criminal using Wite-Out and changing the payee name to their own—others are much more subtle. These more complex schemes, which tend to go after larger sums of money, begin with a fraudster opening an account under a name that is a slight variation of the company’s actual name, such that it may not be noticed by less sophisticated, more manual detection protocols, Booth explained.

From there, they’ll steal or create a check—through the mail, via a corrupt employee, etc.—and they’ll use that similar name on the payee line and cash the check. “It can be very, very subtle—a word might just be spelled wrong. And to the naked eye, it might not look like anything and the check will be cashed, and off it goes,” Booth said.

But if the company has set up payee positive pay, the bank’s system should be unable to match it against acceptable payees listed in its database and the check will be kicked out as an exception to review. “Payee positive pay might be more expensive at some banks, but it’s a very important protection,” Booth said.

Unfortunately, AFP's fraud survey found that only 41 percent of organizations and 55 percent of organizations with revenues over \$1 billion use the service.

But even payee positive pay isn't infallible. Litster noted that forgers are beating the protection today by adding a new, bogus payee name two lines above the original name. Because almost all banks' OCR payee positive pay software looks at a specific X,Y coordinate on the check face for the payee name, as well as the line immediately above the payee, a bogus payee added two lines above the original payee will pass through payee positive pay undetected. He recommends printing a string of asterisks or verbiage, including a secure name font, two lines above the payee name to eliminate any open area where a bogus payee name can be added.

One more protection Booth advises treasury professionals to ask their banks about is what he calls teller positive pay. If a perpetrator visits a branch of the financial institution that issued a check and the teller system is not synced with its back office positive pay system, the check could be negotiated. "That's a subtle thing that corporates should be asking about; whether a bank's teller system is integrated with its positive pay solution," he said.

Holder in Due Course

Holder in due course (HIDC) is an important risk factor treasury professionals need to understand because it can impact an organization's fraud liability and the checks it issues. HIDC refers to anyone who accepts a check, and on the face there is no evidence of alteration or forgery. Under the Uniform Commercial Code (UCC), the recipient of the check is a HIDC and is legally entitled to be paid for the check—even if a stop payment has been placed on it, or if the check was rejected by the bank for any reason, including as a positive pay exception item. "Holder in due course trumps a stop payment and trumps positive pay," Litster said.

If a holder is unable to negotiate the check, they can sue the check issuer (drawer) for the full face value of the check, and get a judgment against the drawer. The statute of limitations to sue is 10 years from the issue date, or three years from the date the check was returned unpaid. A holder also can transfer their rights to the instrument to another party as long as that party wasn't involved with any underlying fraud related to the check. The new holder has the identical legal rights as the original holder, and can sue the drawer for the face value of the check.

All organizations have occasion to issue a replacement check for a check that allegedly was lost or destroyed. A stop-payment order is placed with the bank on the lost check, and a replacement check is issued. Because HIDC trumps a stop payment, to avoid being forced to make payment on a stop-payment check, corporates always should print an expiration date on the face of the check. "If you print, 'This check is void 30 days from issue date, you cut 10 years down to 30 days,'" Litster said. "The key is to keep the expiration date very short. Less than 30 days is preferable, though there are some municipalities that require it to be 60 days."

The only way an organization can ensure that it doesn't end up paying twice is to institute a policy that a replacement check can be issued only after the expiration date has passed on the original check. "If someone accepts a check after that number of days, they have accepted an expired instrument and they have no legal standing as a holder in due course," Litster said, noting that the banks typically pay no attention to expiration dates because they are not obliged to honor them.

Sight Review Paid Large-Dollar Checks

Litster recommends that organizations look at the images of large-dollar paid items—checks made payable to tax agencies such as the IRS, and to charities—as soon as the bank statement is available. The sight-review purpose is to ensure that the payee name has not been altered or a new payee name added.

Under the UCC, an added or altered payee is the liability of the bank of first deposit (BOFD) for one year. However, many banks have implemented "cut-down" provisions for a customer to report any alterations or errors. The cut-down period is often as short as 60 days, and can be even shorter. What's more, tax agencies and charities typically don't give notice of an unreceived payment until well past any bank-established cut-down deadline. "While the BOFD has liability for an added or altered payee for one year, it can take the cut-down provision of the payer bank and enforce that cut-down provision to successfully defend itself," Litster said.

Additional Protections

Segregation of accounts is another way to mitigate check fraud; 69 percent of respondents to AFP's fraud survey use this protection. For example, when Marriott makes tax

“I’ve been here 10 years and we’ve been looking at this for 10 years. We monitor the bank account, we know the size of the checks, and we’ve been able to catch the few checks over the years that came through that account.”

payments it either sends money to the tax authority, or allows the tax authority to debit its bank account. But those are the only payments that are allowed to come out of that account, whether it’s a check or an ACH payment, Wolfe said.

Marriott also uses “post no checks” blocks on any accounts where it would never expect a check to be posted. “It’s another service the banks provide—some charge, some don’t,” Wolfe said.

Sometimes traditional protections are unavailable. In those instances, treasury needs to watch its accounts. Marriott has one particular account for which a positive pay file can’t be created. “The checks are produced out of a system that is not amenable to creating positive pay files at the bank,” Wolfe said. “I’ve been here 10 years and we’ve been looking at this for 10 years. We monitor the bank account, we know the size of the checks, and we’ve been able to catch the few checks over the years that came through that account.”

It also helps if the bank is paying close attention. One check worth \$200,000 nearly slipped through; fortunately Marriott’s bank caught it. “That was one where we could have had a large loss on, but fortunately the bank was on top of it as well,” Wolfe said.

Conclusion

Simply put, checks are here to stay. While corporate treasury professionals should continue to prompt vendors and clients to move to safer and cheaper payment methods, they must take checks seriously. That means investing in the proper protections to thwart would-be fraudsters.

Key Takeaways

- B2B payments by check increased to 51 percent, up 1 percent from 2013 to 2016. Since AFP began its Electronic Payments Survey in 2004, check use has been in decline—until now.
- The recent influx of high profile data breaches and business email compromise (BEC) scams may be causing some corporates and consumers to revert back to checks.
- Legacy systems are another reason why checks are still in play. Many systems are so old that they can only send paper checks.
- Corporates can reduce some check costs by outsourcing the printing and mailing process to the bank.
- Fully 59 percent of organizations experienced between one to five incidents of check fraud in 2016, according to the 2017 AFP Payments Fraud and Control Survey.
- Standard positive pay is a highly effective control. But it is imperative that corporate treasury departments invest in payee positive pay.
- To avoid paying out more than once to a holder in due course (HIDC) check claim, corporates should always print an expiration date on the face of the check.
- Organizations should review the images of large-dollar checks paid to tax agencies and charities as soon as the bank statements are available to ensure the payee name has not been altered.



About the Author

Andrew Deichler is the editorial manager for the Association for Financial Professionals (AFP). He produces content for a number of media outlets, including AFP Exchange, Inside Treasury, and Treasury & Finance Week. Deichler regularly reports on a variety of complex topics, including payments fraud, emerging technologies and financial



Magnus Carlsson is the manager for treasury and payments at the Association for Financial Professionals (AFP). Previously, Carlsson worked as the project manager for the SEPA project at AB Volvo and was the arbitrage manager for the Arlington County Treasurer’s Office, managing all arbitrage issues, debt service payments and investment management. He was with the Federal Home Loan Banks (FHLB) Office of Finance for seven years in positions of increasing responsibility and scope including credit analysis, short-term debt issuance and investor relations.



ASSOCIATION FOR FINANCIAL PROFESSIONALS

About the Association for Financial Professionals®

Headquartered outside Washington, D.C., the Association for Financial Professionals (AFP®) is the professional society that represents finance executives globally. AFP established and administers the Certified Treasury Professional® and Certified Corporate FP&A Professional™ credentials, which set standards of excellence in finance. The quarterly AFP Corporate Cash Indicators® serve as a bellwether of economic growth. The AFP Annual Conference is the largest networking event for corporate finance professionals in the world.

General Inquiries: AFP@AFPonline.org
Website: www.AFPonline.org
Phone: 301.907.2862



Your trust, your future, our commitment

MUFG, a major multinational financial group, offers comprehensive and tailored financial solutions to our clients around the globe. With more than 350 years of history, \$2.6¹ trillion in assets, and operations in nearly 50 countries, MUFG is steadfast in its commitment to serving business and society by building long-term client relationships. Focused on your future, we work every day to earn your trust.



MUFG Union Bank, N.A.
A member of MUFG, a global financial group

¹ Exchange rate of 1USD = ¥116.49 (JPY) as of December 31, 2016.
©2017 Mitsubishi UFJ Financial Group, Inc. All rights reserved.
The MUFG logo and name is a service mark of Mitsubishi UFJ Financial Group, Inc., and is used by MUFG Union Bank, N.A., with permission. Member FDIC. mufgamericas.com