

# Global Treasury Management

WELLS  
FARGO

## Secure Payables Discussion

May 1 2023

---

Will Taylor, Relationship Manager  
Kristen Cooper, Treasury Management Consultant  
Carl Williams, Payables Consultant

# Fraud is imminent, will you be...

susceptible

with impacts to

- revenue
- proprietary data
- trust
- reputation
- relationships
- employees
- regulations

or

prepared



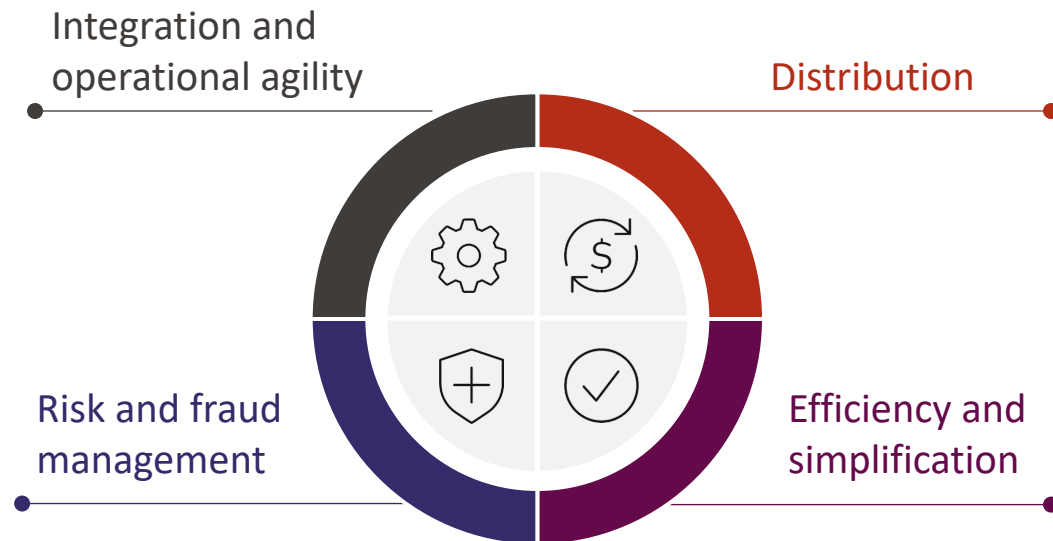
# Improving disbursement efficiency: Government entities



We understand that as a state or local government, managing day-to-day payments can be challenging, as you're often asked to distribute large amounts of money in a relatively short amount of time.

But there are processes you can put in place to help **make disbursements easier and manage risk**.

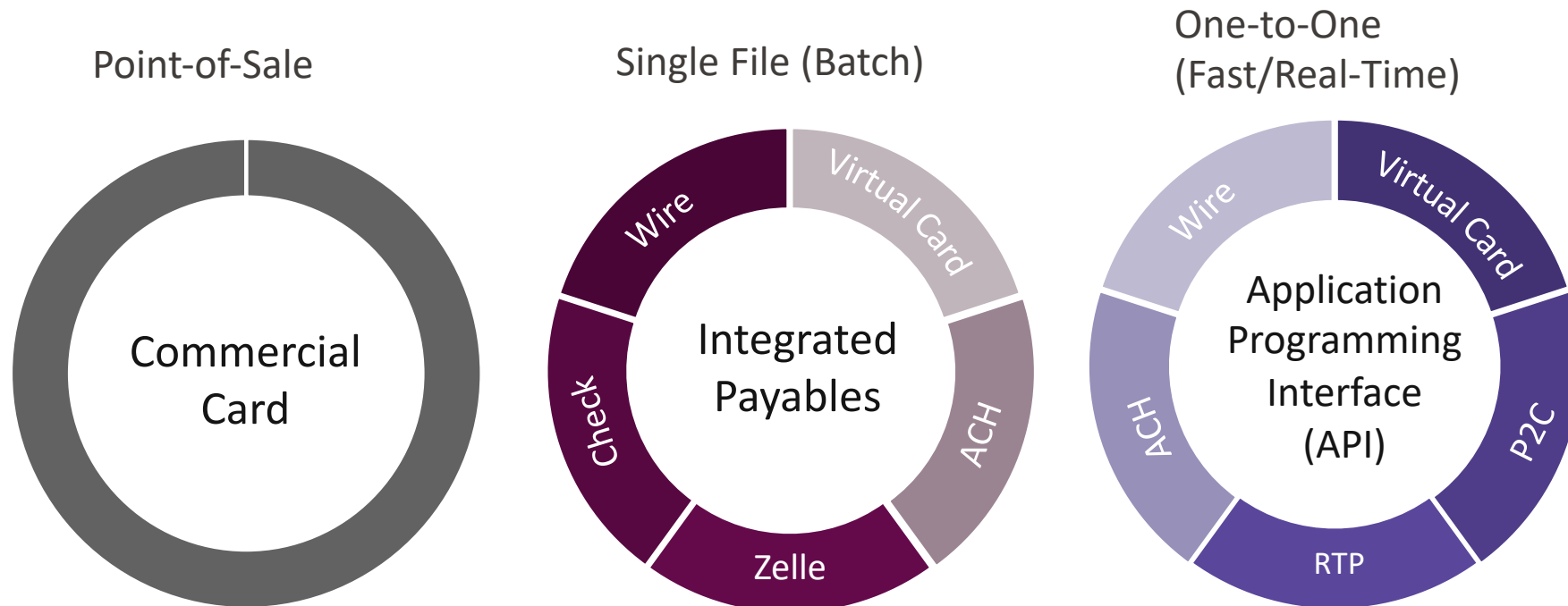
The right combination of services can help you improve:



Distribute funds to your constituents in a way that can be faster for them and easier for you.

# Shifting to electronic options

In today's environment, companies want to pay electronically and suppliers/payees want to be paid electronically. How do you choose how to pay?



\* Zelle and Push-to-Card are Business-to-Consumer payments



# Faster payments comparison

	Same Day ACH	Disbursements with Zelle®	Wire	Push to Card	RTP® Services
	Fast 5:00 p.m. local time or earlier	Faster Near real time to 3 days <sup>1</sup>	Even faster Near real time for domestic	Fastest Within minutes	Instant Real time
Business models	B2C, B2B, C2B	B2C , B2smallB	B2C, B2B, C2B	B2C, B2smallB	B2C, B2B, C2B
Remittance	9,999 addenda records; 80 characters remittance data each <sup>2</sup>	Optional 140-character description on payment notification	9,000 characters	18 characters on payee card statement + 6–25-character payment reference ID	140 characters in payment message + extensive remittance advice
<b>Origination information</b>	<b>Routing and account number</b>	<b>Email or U.S. mobile phone number</b>	<b>Routing and account number</b>	<b>Debit card</b>	<b>Routing and account number</b>
Settlement finality	Depends on reason for return, can be up to 60 days	Irrevocable; can support request for return <sup>3</sup>	Irrevocable; can support request for return <sup>3</sup>	Irrevocable; can support request for return <sup>3</sup>	Irrevocable; can support request for return <sup>3</sup>
Posting	Same day as a settlement	Real time	Real time	Real time	Real time
Maximum transaction limit	\$1,000,000	\$50,000	\$9,999,999,999.99	\$10,000 standard; up to \$50,000	\$1,000,000

1. Enrollment required. Terms and conditions apply. Payments can arrive as quickly as minutes or may take up to three business days after payment is sent. Must have a bank account in the U.S. to use *Zelle*. For your protection, *Zelle* should only be used for sending money to trusted recipients.

2. 14 characters are reserved for record type and addenda sequence.

3. Return of funds is not guaranteed.

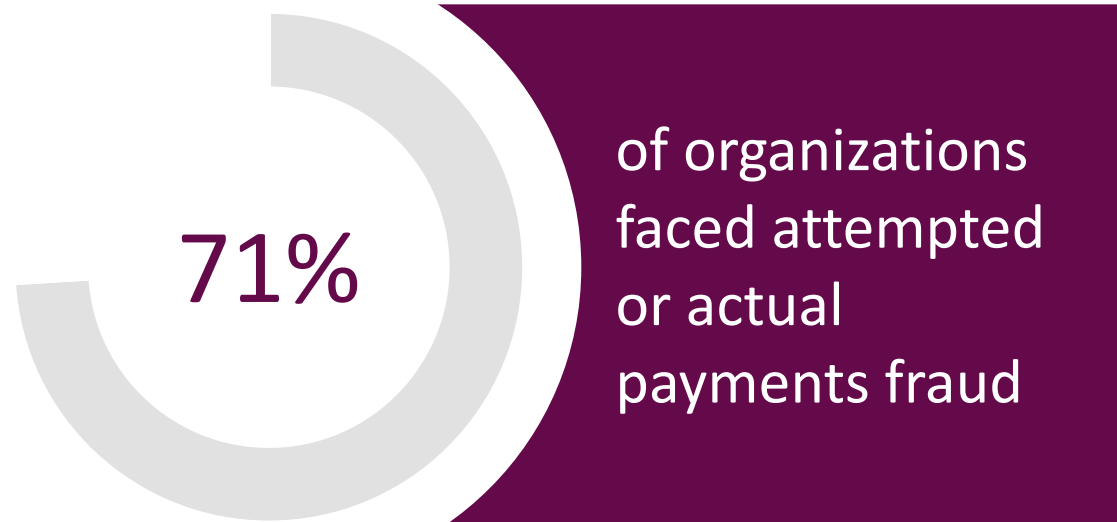
RTP® is a registered service mark of The Clearing House Payments Company, LLC.

Zelle and the Zelle related marks are wholly owned by Early Warning Services, LLC, and are used herein under license.

# Payment fraud continues to be a significant business risk

It only takes one incident for your organization to be compromised

## 2021 fraud statistics



Companies of all sizes, across all industries are at risk

What are you doing to reduce your exposure?

# Are your payments a target for fraud?

Organizations that experienced fraud in 2021 by payment type

---

ACH credits

24%

Corporate/Commercial credit cards

26%

Wire transfers

32%

ACH debits

37%

Checks

66%

# Current threat landscape

Key fraud threats impacting Wholesale customer-facing digital channels

B  
E  
C

## Business email compromise (BEC) aka imposter fraud

BEC is where a fraudster impersonates a vendor, company executive, or another trusted trading partner — ultimately tricking you into making the payment to them.

A  
T  
O

## Online account takeover (ATO)

Cyber criminals access your online accounts to make unauthorized transactions, including transferring funds, or stealing sensitive customer information.



# Business email compromise (BEC) – aka Imposter fraud

Sophisticated fraudsters + time and patience = significant losses

## How they target you

- Spoofed email address
- Compromised email account

## Why it works

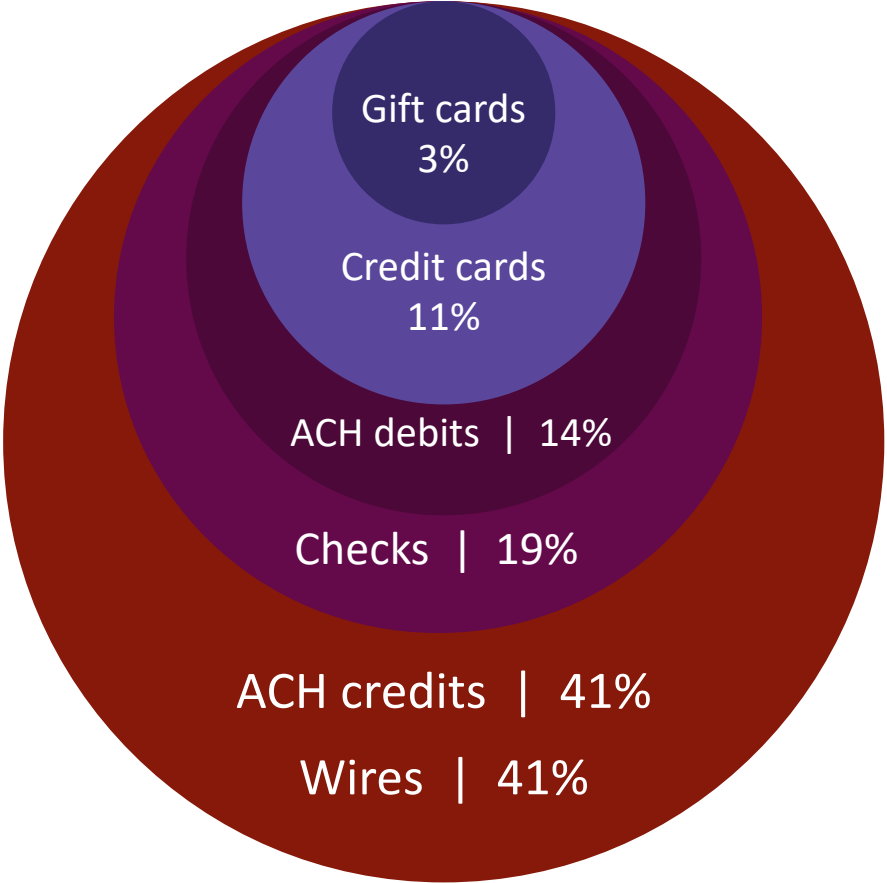
- Attempts appear legitimate at first

## Types of imposter fraud

- Executive
- Vendor
- Payroll

# Payment methods impacted by BEC

Percentage of organizations impacted by payment type



**Wire transfers** continue to be a prime target for BEC scams with 41% of financial professionals reporting impacts with **ACH credits** growing from 34% last year to match wires at 41%

# Steps to help protect against BEC fraud



## Verify the request

- Watch for red flags, especially if a request seems out of the ordinary
- Verbally verify and confirm the request
- Only use the contact information you have in your system of record



## Implement dual custody

- Serves as a second chance to identify potential fraud
- Verify changes and pay attention to the details
- Confirm changes are verified before approving payment



## Monitor accounts

- Reconcile bank accounts daily and pay close attention to account activity
- Protect your email account and login credentials

# What is phishing?

Phishing is the fraudulent attempt to obtain sensitive information, such as usernames, passwords, and account details, typically through an email, text message, or even a phone call.


From: WellsFargo – Support\_Online [WellsOnlineBank2@comcast.net](mailto:WellsOnlineBank2@comcast.net) **1**

Date: December 8, 2017 at 2:23:01 PM EST

To: Undisclosed-Recipients::

Subject: Alerts! **2**

---

 [wellsfargo.com](http://wellsfargo.com)

---

## Security Information Regarding your Account.

We are sorry, For your protection and security reasons, your Wells Fargo account has been locked.

Please click on the following link to unlock your acco **3**

Log-in to :<https://www.wellsfargo.com/online-banking/updating> **4**

Thank you for bringing this matter to our attention.

Sincerely, Wells Fargo Online Banking Team.

[wellsfargo.com](http://wellsfargo.com) | [Fraud Information Center](#)

1. The sender's email address uses an inappropriate domain name
  - In the example, the email domain is “comcast.net” not “wellsfargo.com”
2. The includes an urgent call to action in the subject line and the message copy
3. Phishing emails may also contain extra spacing or unusual punctuation, grammar, capitalization, or language
4. It contains a suspicious link that could lead to a fraudulent website
  - When using a laptop or desktop computer, check the link's URL by hovering over it with the cursor. The URL will show in the browser window

# Account takeover (ATO)

Fraudster steals confidential information to access online accounts directly



- Fraudster typically leverages social engineering and malware to execute an account takeover incident
- Social engineering, such as phishing, manipulates you into divulging confidential information
- Malware is malicious software installed on your computer without your consent or knowledge
- Malware allows a fraudster to access accounts and send unauthorized payments

# Steps to help protect against ATO fraud

## Don't



- Don't share online banking credentials
- Don't click on links or download programs or attachments in emails or text messages, unless they're from a trusted sender

## Do



- Use notification and alert services to receive text or email notifications regarding electronic debits from your accounts
- Implement dual custody
- Use multi-factor authentication, or at least two-factor authentication, for access to your company networks and for payments initiation
- Keep antivirus software current on all your work devices and on any personal devices that you use to access your company's networks
- Install all system and application updates for patching security flaws in timely manner

## Caution



- Be wary of **unsolicited phone calls** concerning unreported system issues – Immediately contact your Wells Fargo bank representative

# Steps to help protect against payments fraud



Dual approval for high-risk transactions



Positive pay and ACH fraud filter



Account validation services



Mobile access to fraud features



Employee training and increased awareness

# Internal control methods for ACH fraud

## Establish rules and outline responsibilities

### Recommended practices

- Document procedures on vendor validation process for new or updated relationships
- ACH debit controls
- Utilizing account validation services
- Daily reconciliation





# Outsourcing supplier analysis and onboarding

## Faster migration

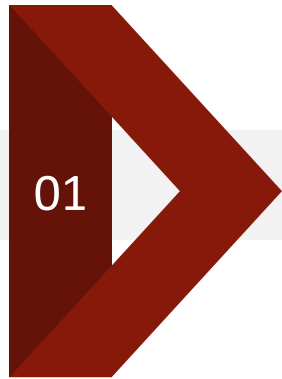
Outsourcing supplier outreach efforts to experienced professionals provides faster migration to electronic payments. Work with a provider performs the task of supplier conversion.

## Committed team

Selecting a project leader on your side to champion the effort and keep in contact with your provider and keep your team up to date.



# ACH enrollment – what controls are offered



Primary  
contact



Add secondary  
contact and direct  
deposit account  
(DDA)



Test deposit  
to DDA



Both contacts verify  
test deposit

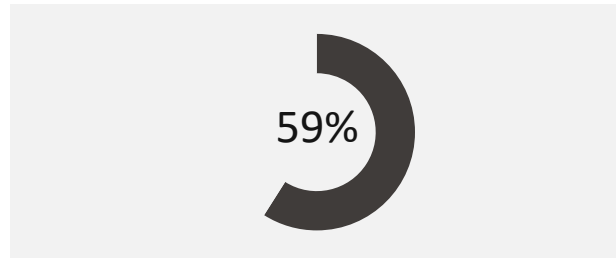
Vendor banking data can be:

- Stored by provider
- Transmitted back to your system securely

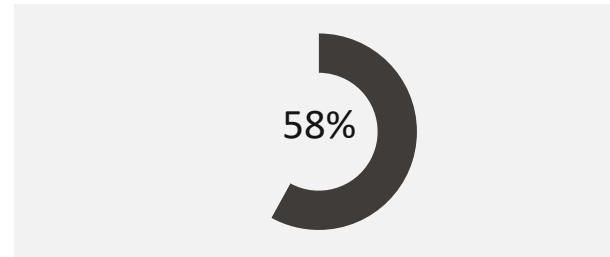
# Internal control methods for ACH fraud

Percentage of organizations leveraging fraud control procedures and services

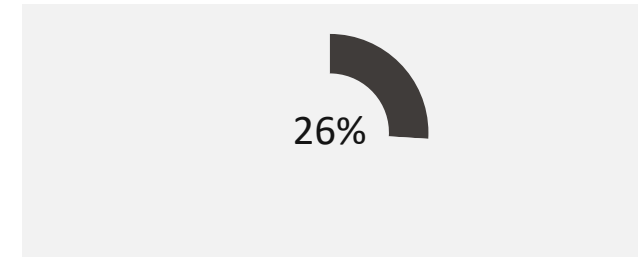
Daily reconciliation



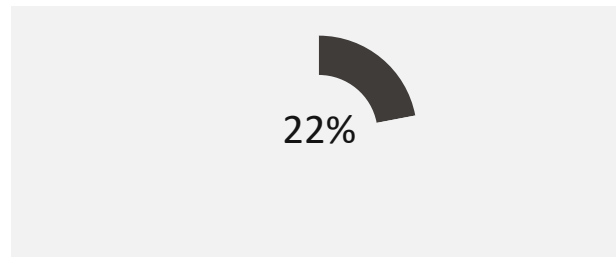
Allow ACH debit on one account set up with ACH debit filter or ACH positive pay



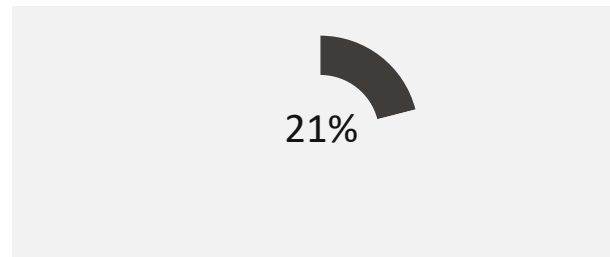
Block ACH debits on all accounts



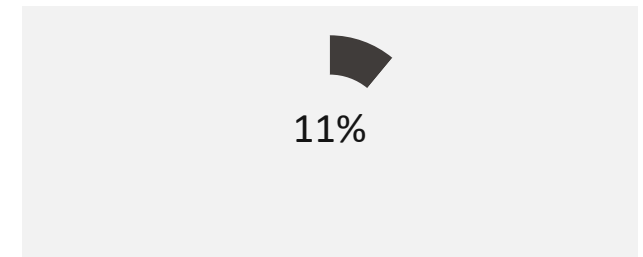
Create separate account for electronic debits initiated by third party



Debit block on all consumer items with debit filter on commercial ACH debits



Minimize use of ACH



# Internal control methods for check fraud

## Establish rules and outline responsibilities



### Recommended practices

- Positive pay
- Payee validation
- Daily reconciliation
- Segregation of accounts
- Check block for non-disbursing accounts

# Know your organization's critical needs

- One size does not always fit all: integrate your security measures to reflect your organization's priorities
- Have an actionable plan in place to respond in case of a fraud attack
- Simple processes can be some of your most powerful safeguards



# Education and awareness to help mitigate the risk

## Educate your entire staff

### Create a cyber security culture

- Establish a regular and ongoing process for educating staff
- Instruct all staff, especially AP staff, to question unusual payment or account change requests received by email — even from executives
- Alert management and supply chain personnel to the threat

## Vendor and trading partner awareness

### Share your knowledge and best practices

- Educate your vendors and trading partners—they are targets for fraud, too
- Define a communication process for payment and account changes

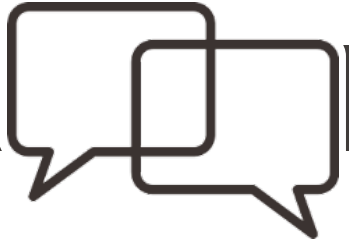
# Resources for more fraud protection information

## Wells Fargo fraud websites for additional fraud assets

- Treasury Insights Fraud & Security page  
<https://global.wf.com/treasury-insights/fraud-security/>
- Wellsfargo.com fraud page  
<https://www.wellsfargo.com/com/fraud>

## External resources

- FBI Internet Crime Complaint Center (IC3)  
<https://www.ic3.gov>
- Cybersecurity & Infrastructure Security Agency (CISA)  
<http://www.cisa.gov/>



Q&A