


| | | | |
|--|-------|---|-------|
| INSIDE: Rules Recap - 2018 ACH Rules Changes..... | pg. 1 | 5 Things Most Small Businesses Don't Know About Credit Card Payment Processing..... | pg. 5 |
| Business Email Compromise - Be on the Look Out for These Scams | pg. 1 | 20 Cash Handling Best Practices Your Business Should Follow..... | pg. 5 |
| Does Your Business Issue Remotely Created Checks?..... | pg. 1 | Toolkit Can Help You Grow Your Nonprofit with the Help of Direct Deposit..... | pg. 6 |
| How Same Day ACH Can Be Advantageous for Small Businesses..... | pg. 2 | Older Americans Month 2018: Engage at Every Age..... | pg. 9 |
| SWIFT Reveals Success, Future Challenges of Blockchain PoC..... | pg. 3 | | |

Rules Recap - 2018 ACH Rules Changes

Same Day ACH: Moving Payments Faster, Phase 3

Phase 3 Effective March 16, 2018
Phase 3 of The Same Day ACH: Moving Payments Faster rule (Rule) builds upon the foundation established by the earlier phases of Same Day ACH. The implementation of Same Day ACH is completed with Phase 3, where most RDFIs are required to provide funds

availability for same day credits by 5 p.m. RDFI local time.

Impact to Corporate Users: Businesses should discuss Same Day ACH with their financial institution to determine whether it is appropriate and cost effective. Businesses receiving Same Day ACH credits should contact their financial institution with funds availability questions. 

Business Email Compromise - Be on the Look Out for These Scams

by Karen Sylvester, AAP, CAMS, CRCM, NCP, Director, Regulatory Compliance

You have probably heard about those emails that claim to be from the big boss and which often start off with a line similar to this, "I need you to do something for me." Frequently there is also a sense of urgency inferred that makes the average worker bee jump to attention when such an email hits their inbox. Unfortunately, criminals have figured out that impersonating a person in authority at an organization, or even a known vendor

to whom you may remit payments, often results in action being taken that benefits the criminal. Let's look a few different ways this fraudulent scenario may play out, as well as a few tips on how to protect your organization from falling victim to these crimes.

The Email from the Boss

With a quick glance, an incoming email appears to be from the CEO, Joe Smith. Joe is asking you to send a wire of \$25,000 immediately to pay for a shipment that needs to go out today. In the email, Mr. Smith tells [see EMAIL on page 3](#)

Does Your Business Issue Remotely Created Checks?

by Marcy Cauthon, AAP, NCP, Director, On-Demand Programs

As of July 1, 2018, new Federal Reserve Board Regulation CC amendments go into effect. These amendments define a new type of check. An Electronically Created Check (ECI) is a check-like item created in electronic form that never exists in paper form. This new definition could qualify some of the Remotely Created Checks (RCC) that your business creates today as an ECI instead of an RCC.

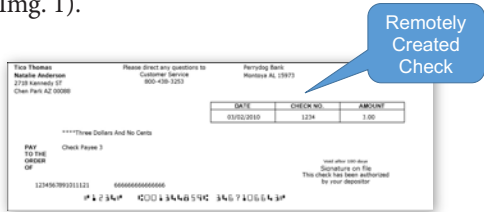
The RCC definition in Regulation CC states:

"A Remotely created check means a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn."

This definition implies that an RCC is a paper item that does not bear the account holder's signature. By comparing the definition of an ECI versus an RCC the [see CHECKS on page 2](#)

CHECKS continued from page 1

difference is that one is in paper form while the other never is printed in paper form (see *Img. 1*).



Img. 1

It is known in the check industry today that there are times when businesses do not print Remotely Created Checks but digitally create these items based on account information provided to them by an account holder. If your business creates these items electronically and can transmit them to your financial institution electronically and your financial institution can process electronically, this scenario would qualify these items under the ECI definition, not the RCC definition.

While the newly defined ECI might sometimes contain a signature where the RCC does not (some software platforms can generate an electronic signature on these items – see *Img. 2*), the significant difference is in the processing of the check. How your

business is transmitting the item to your financial institution will determine what type of items you are truly processing.




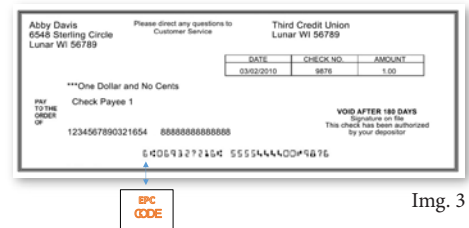
Img. 2

The most important thing to stress is that your business must have an agreement in place with your financial institution in order to process Remotely Created Checks or Electronically Created Items. These agreements are important as there are warranties on both types of items. The warranties include:

1. Your business received the account holder's authorization to create the item;
2. The item was created based on account information the account holder provided you (routing number, account number, next check number); and
3. Your business printed the RCC or digitally created the ECI based on account information provided.

Financial institutions receiving unauthorized returns for these items will charge the item(s) back to your business, therefore possibly resulting in a loss to your business. Proper authorization in creating these types of items is pivotal in helping prevent such losses.

A couple of years ago, the industry developed a new External Processing Code (EPC) code for businesses to utilize on the MICR line of their RCC items (see *Img. 3*). This is an optional 1-digit field of a "6" which is located to the left of the routing number on the RCC. The code is optional, however; it may be important to start utilizing this field more to distinguish an ECI vs. an RCC. As the industry continues to evolve, an EPC code for ECIs may also be developed and the EPC may become a mandatory field for these types of items. 



Img. 3

How Same Day ACH Can Be Advantageous for Small Businesses

Do you use ACH transactions as part of running your small business? You do if you provide a direct deposit option for payroll, if you make electronic payments to the government for payroll taxes, if you use online banking to make bill payments, receive customer-initiated online banking payments for your invoices or if you process direct debits from your customers' bank accounts. (If you don't, you're missing out on a major convenience and potential cash flow improvement—talk to your financial institution or your payroll processor to learn more.)

If your business does use ACH, you've probably heard about Same Day ACH. For

businesses and consumers alike, it means the ability to move money faster, which is in most cases a good thing. But, will Same Day ACH help your small business operate more efficiently? If your business can benefit from sending and receiving funds more quickly, and the benefit warrants paying a premium for it, then Same Day ACH will be a welcome enhancement.

ACH Basics

Before delving into the Same Day ACH topic, let's begin with some ACH basics. ACH stands for Automated Clearing House,

which is the network via which money moves between banks. At its very simplest, an ACH transfer is a command to move funds from one bank account to another.

The main advantage of ACH over paper checks is processing time—when a transaction is electronically transmitted to the banking network it removes a number of intermediary steps (such as mailing a paper check, picking up the mail, creating a deposit, etc.) that can delay the availability of funds. With traditional ACH, funds are typically made available to the recipient 1-2 business days after the transaction enters the ACH

[see SAME DAY on page 4](#)

SWIFT Reveals Success, Future Challenges of Blockchain PoC

SWIFT (Society for Worldwide Interbank Financial Telecommunication) has offered another update on its blockchain proof of concept (PoC), reiterating its potential to enrich transaction data, support real-time liquidity management and reconciliation and more.

In an announcement in early March, SWIFT said its DLT (distributed ledger technology) PoC for Nostro reconciliation went “extremely well,” according to SWIFT Head of Research and Development Damien Vanderveken in a statement.

“The DLT sandbox enabled us to control access, to define and enforce user privileges, to physically segregate confidential data and store it only with the relevant parties while supporting a strong identity framework by linking all participants to their BI and having

all keys signed by a SWIFT certification authority,” added Vanderveken.

The PoC includes 34 banks, each with their own node in SWIFT’s DLT sandbox. The solution deploys Hyperledger to assess the potential for blockchain to enhance bank-to-bank transactions.

“The PoC sought to assess whether DLT, combined with SWIFT assets, would meet industry-level governance, security and data privacy requirements, whether DLT could bring concrete benefits over other architectures and to check DLT’s current level of maturity to serve as a production-grade application within a mission critical global infrastructure,” SWIFT said in its announcement.

The tool uses ISO 20022 payments messaging standards and technologies that are part of SWIFT’s GPI (global payments

innovation) initiative combined with blockchain technology to enable the recording of transactions linked to Nostro Accounts.

While SWIFT said the PoC was successful, it also highlighted some challenges to adoption.

“Although the PoC demonstrated DLT could improve Nostro liquidity management and reconciliation processes, it also revealed that the prerequisites will have to be met before banks can enjoy the full benefits of switching to a DLT process,” said Vanderveken.

Among those prerequisites include migration from batch to real-time liquidity reporting, while financial institutions would have to upgrade back-office applications to enable a real-time data feed to the DLT platform. 📍

Source: PYMNTS.com

EMAIL continued from page 1

you he will be in meetings all day, so you sense the urgency and the importance. Mr. Smith was even kind enough to send you all the wire details including routing and account information and the beneficiary’s information. Without a second thought you create the wire and have a coworker approve it in your online banking platform. A few hours later, you see Mr. Smith in the breakroom and let him know the wire was sent out just as he requested. Your first sign of trouble is the puzzled look on his face. Upon closer review of the email, you see the email came from Jo Smith but your CEO’s actual email address is Joe Smith.

Vendor Payment Details

EHN Company has been a longtime vendor with your organization, and they send invoices via email which you process payment for on a daily basis. EHN’s new employee, Ken Jones, introduces himself via

email, and goes on to explain that he has been tasked with updating EHN’s processes and procedures. Through several emails back and forth, you kindly share how your process works and how well it has been working for the last few years. A few days later, Ken sends an email requesting that EHN’s payment remittance information be updated to a different financial institution—with a new routing number and account number. You thank Ken for helping you keep your information up-to-date, and, when the next invoice from EHN is emailed to you, you process the payment to the updated account. A few days later, ENH sends you another invoice claiming non-payment. You inform them that you submitted the payment to the updated account information provided by Ken Jones. ENH responds they did not update their remittance account information, and they’ve never heard of Ken Jones.

These are just two examples of how

organizations are falling victim to this type of crime which has been coined “Business Email Compromise” or BEC. In both of the previous scenarios, the crime may have been stopped if there were more controls in place.

As you review your internal processes, these are a few questions you may want to ask:

- Who within your organization can request a payment to be sent?
- How are those requests sent?
- What approval process do you have for payment requests?
- What procedures do you have in place to update account information for your vendors?

As technology advances, so do the ways that criminals try to infiltrate our systems and access money that does not belong to them. The use of external confirmation procedures and taking a few minutes to ask yourself, “Does this make sense?” could save you from falling victim to this type of scam. 📍

SAME DAY continued from page 2

network. With Same Day ACH those funds can be made available on the same day the transaction enters the ACH Network.

There are two basic types of ACH transactions—those where money is pushed (ACH credits) and those where money is pulled (ACH debits).

The most popular types of ACH credits are payroll transactions and online bill payments (i.e. a credit card bill payment, a utility bill payment, or any other payment to a vendor or service provider).

With an ACH debit, customers provide a business with their bank account information along with authorization to process one-time or recurring transactions for a specified amount (the business never has to disclose its own bank account number). The business then initiates an ACH debit to pull money from its customers' accounts into its own. To use ACH debits, a small business must typically obtain an ACH merchant account directly from their bank, or from a third-party provider.

The Cost of Same Day ACH

With nothing in life being free, financial institutions may charge for this premium service to their business customers initiating Same Day ACH transactions. Third-party processors will likely also offer Same Day ACH for an added fee, and likely Same Day ACH settlement for an even higher fee.

As a small business owner, you'll need to balance the advantages of sending and receiving funds sooner against these added costs. In many cases, traditional multi-day

ACH transactions will be just fine. In others, particularly when you avoid a hefty fee for late payment, it can be well worth the cost.

Advantageous Uses of Same Day ACH Credits for Your Small Business

Getting paid more quickly is a clear advantage to using Same Day ACH for debits, but there are significant cash flow advantages



to using it for ACH credits as well.

For example, with traditional ACH, funds are withdrawn from your account up to three business days before they are deposited into the recipients account—be that recipient an employee or a vendor. With Same Day ACH you can keep your money longer. (Though with the paltry interest rates currently available, the cost of money is rather negligible.)

Same Day ACH can also help you avoid late fees if you forget to make a payment; can enable you to process emergency payroll; and can even enable you to process payroll for hourly workers without having to guess at hours worked.

The ability to offer same day payment to your own vendors and service providers may enable you to get more advantageous pricing


from them—and that savings may offset the costs of paying early and even the costs of processing the Same Day ACH transactions.

Getting Your Small Business Ready for Same Day ACH

The best thing you can do to prepare your small business for Same Day ACH is to speak with your service providers and with your financial institution. If you're interested in using Same Day ACH credits for payroll, now is the time to have that discussion with your payroll provider. Likewise, if you see benefit from being able to initiate Same Day ACH debits, talk with your financial institution to see if they offer Same Day ACH and determine if this option is cost-effective for your business.

Same Day ACH Resources for Small Businesses

NACHA—the governing body for the ACH Network—has created a website dedicated to Same Day ACH. Check out the [Same Day ACH Resource Center](#) for a large library of materials on the upcoming change. One key resource is the *Same Day ACH for Businesses Essentials Guide*, which helps you understand the upcoming changes, how exactly they will be implemented, and how they can benefit your small business.

If you're interested in payroll applications of Same Day ACH see [Guidance for Employers and Payroll Professionals on Same Day ACH Direct Deposit](#). 

Source: [PaySimple.com](#)



IF YOU WANT TO BE THE BEST, YOU HAVE TO TRAIN WITH THE BEST!

The pass rate for participants of EPCOR's AAP Prep Program consistently beats the national average. Start training on May 15 to get in tip-top shape for the Accredited ACH Professional (AAP) exam this Fall! Visit [epcor.org](#) for details.

5 Things Most Small Businesses Don't Know About Credit Card Payment Processing

What you don't know can hurt you when your small business handles sensitive payment data. In fact, ignorance of the risks and responsibilities associated with payment processing can result in your business being exposed to possible fines, fees and operational upheaval.

Here are five things most businesses don't know about payment processing.

Processing Type Impacts the Level of Payment Protection

Most debit and credit cards that were re-issued in the United States in 2015 to include EMV chips now include a magnetic strip on the back and an EMV chip on the card's front. Yet, many businesses don't know there are significant differences in payment security when a card is swiped versus inserted into the EMV payment terminal.



When a customer uses the EMV chip card feature, the processing environment utilizes a security measure called tokenization. This process replaces the sensitive cardholder data (i.e., the 16-digit personal account number) with a series of randomly assigned numbers used to process the payment. If the

transaction is intercepted during processing or later compromised in a breach, data thieves cannot use the token to commit further fraud or identify the account owner.

You Are Not Too Small for a Payment Security Breach

According to a recent cybersecurity article in Forbes, nearly 20% of small businesses have been impacted by a security breach. Credit card processor First Data estimates that most small businesses that are victims of a payment security breach don't know it occurred until the damage has been done. If a breach does occur, mandatory investigative audits of payment security practices cost the average small business about \$36,000, according to First Data.

see **PROCESSING** on page 6

An advertisement for the 2018 NACHA Operating Rules & Guidelines. It features a hand holding a glowing smartphone that displays the book cover. The cover text includes '2018 NACHA Operating Rules & Guidelines' and 'The Guide to the Rules Governing the ACH Network'. Below the image, it says 'Order Your 2018 ACH Rules Today!' and 'Now featuring an App option and online-version with increased search functionality! Relying on outdated Rules can cause confusion and hinder compliance!'.

20 Cash Handling Best Practices Your Business Should Follow

Small businesses that deal in cash like food trucks and salons need to protect themselves against errors involving cash and theft. Here's 20 cash handling best practices your business should follow so everything runs smoothly.

Eliminate Slush Funds

Cashiers in small retail stores are often expected to make up for shortages from their own pockets. This can lead to an employee slush fund to pool resources. It's generally a bad idea that can hide the real reason the drawer goes short. If you use one of these, get rid of it.

Be Strict About Differences

A few dollars short here and there might not seem like a big deal at first in a small

diner that has a good lunch crowd. However, ignore discrepancies and you might be glossing over a bigger issue. Recording all losses and overages helps to uncover anything deliberate.

Standardize a Process

Everyone needs to be on the same page when staff is handling cash on your small fleet of food trucks. Putting together a one-size-fits-all set of rules takes the guesswork out of handling cash for employees that work autonomously.

Know the IRS Obligations

You need to know what the [government expects](#) as far as cash transactions go.

see **CASH** on page 7

PROCESSING continued from page 5

If you are party to a payment transaction found to have offered the lowest level of security, you could be held responsible for costs associated with the breach, including identity protection services for breach victims, the cost of card re-issuance, fines and legal fees.

Now that the October 2015 deadline for transitioning point-of-sale equipment to be compliant with EMV card chip technology has come and gone, merchants who don't accommodate EMV chip cards could be held liable in the event of a payment security breach.

You Need a Multipronged Approach to Payment Security

Choosing a payment processor that guarantees PCI-compliant payment processing and accommodating EMV chip card technology at the point of sale are two ways to enhance payment security, but you cannot rely on one method in isolation. Your business needs to conduct its own audits to proactively identify vulnerabilities and potentially adapt those processes as your business grows.

For example, the PCI compliant security standards set forth by the [PCI Security Standards Council](#) outline the specific protocol merchants should follow based on the volume and type of annual transactions. At a minimum, internal audits of firewalls, networks, hardware and software should take place quarterly, under PCI-compliant processing standards.

Not All Payment Security Issues Originate with Cybercrime

Not all breaches occur with a sophisticated hack. In fact, Computerworld reports that the 2013 Target payment security breach originated with valid log-in credentials from the company's HVAC vendor that were not properly safeguarded.

Your internal procedures make a significant impact on payment security. Passwords should not be posted on computers or at point-of-sale systems, should be changed at least every few weeks and should consist of eight characters including letters (upper and lower case), numbers and symbols.

Your Staff Plays a Critical Role in Payment Security

One employee's innocent mistake can make or break your payment security and cost your business dearly. Conduct ongoing training sessions to ensure secure payment procedures. For example, customer credit or debit card numbers should never be written down or kept on file.

Mobile payments should be processed only with a secure and password-protected connection, using the mobile payment provider's secure app or provided dongle. The operating system of any mobile device used to process payments should be updated to reflect the most recent version (which is often patched when security vulnerabilities are detected).

Payment security is an important issue for any merchant that handles sensitive data. The more you understand how to provide a secure environment in your technology and internal processes, the less you risk you face as a business. 🍀

Source: *Business.com*

Toolkit Can Help You Grow Your Nonprofit with the Help of Direct Deposit

NACHA, the governing body of the ACH Network, has created a nonprofit toolkit, designed to help nonprofits grow their sustaining donor programs. The toolkit offers practical tips and resources for leveraging direct withdrawal *via ACH*—a form of Direct Payment *via ACH*—to retain donors and sustain contributions.

The [nonprofit toolkit](#) consists of four core pieces:

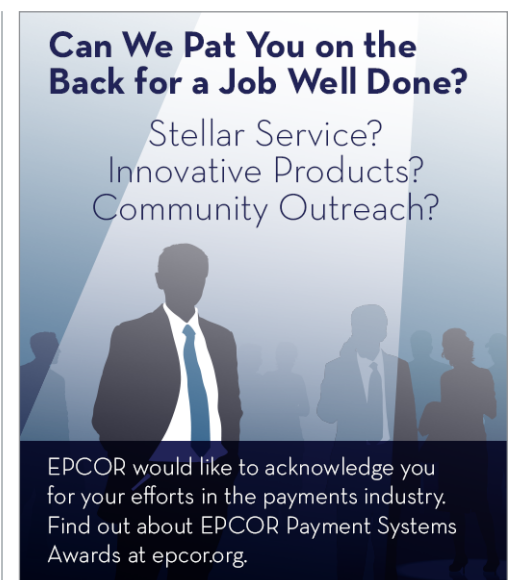
Case Study – Featuring Capital Public Radio's "Evergreen" campaign, this case study provides a concrete example of how ACH payments increase donor contributions and

retention. The station reports ACH payments are responsible for more than 40% of all individual donation dollars, and they retain ACH donors up to 20% longer than those using credit cards.

Checklist – Identifying specific steps, this checklist simplifies the process of establishing a sustaining donor program with ACH.

Best Practices – Once established, nonprofits can enhance and grow their sustaining donor programs by increasing ACH payments. This document outlines tried-and-true practices that deliver increased sustainer donations for nonprofits.

[see TOOLKIT on page 8](#)



Can We Pat You on the Back for a Job Well Done?

Stellar Service?
Innovative Products?
Community Outreach?

EPCOR would like to acknowledge you for your efforts in the payments industry. Find out about EPCOR Payment Systems Awards at epcor.org.

CASH continued from page 5

There's no way around performing your due diligence. For example, large cash payments over \$10,000 need to be handled a certain way. If you're in doubt, check with the IRS or your accountant.

Have a Petty Cash Account

Having some petty cash on hand to make change for customers in your laundromat makes for a great competitive advantage. Opening a business checking account to fund one keeps your bookkeeping above board.

Issue Invoices

It's not a problem when regular clients want to pay in cash at your nail salon. You only need to issue them an invoice.

Don't Mix Up Accounts

All the cash your business handles needs to be recorded and stored separately and proper bookkeeping procedures need to be followed. For example, never take some customer cash payments to replenish petty cash.

Have a Schedule for Handling Cash

If you run a small retail outlet in the local mall, your days might be hectic. Depositing, counting and balancing your cash should follow a strict schedule. Work that routine around your busy times of day.

Have Upper Limits

Avoiding theft and lost monies is also about keeping a limit on how much you keep in the registers and on hand. Keeping this simple means having an upper ceiling on how much you have on site.

Invest in Cash Technology

Smart safes make the job of handling cash more efficient. These track cash transactions and can even schedule pickups. Counterfeit detection technology is another must have for cash businesses like smaller restaurants.

Limit the Employees Who Handle Cash

Effective cash management starts with assigning the responsibilities to supervisors. They should be responsible for reviewing transactions and other duties like recording receipts.

Don't Share Cash Drawers

Mistakes happen in restaurants and retail stores when people share a common cash drawer. It might be convenient in a restaurant to have a waiter cover someone who is on break, but there's a lack of accountability there. Everyone should have their own assigned cash drawer.

Don't Round Numbers Off

It's called dollars and cents for a reason. David S. Peters is an expert on the subject in the restaurant world. He says rounding off the nightly deposit by leaving coins out can only lead to accounting headaches down the road. Don't try and save time by avoiding loose change.

Use Accounting Technology

Using the latest technology can help you manage the cash for your hardware store. Don't assume the big names in accounting software only cater to the big box stores in your field. For example, QuickBooks makes setting up a petty cash account easy.

Tweak the Process Continually

You should always have an eye to improving your cash handling systems. That includes changing the responsibilities you assign to employees as you see fit.

Concentrate on Counting

You might even be a sole proprietor on a busy food truck. If you're handling cash transactions, you need to concentrate. If you get interrupted, always start over again from the beginning when counting.

see CASH on page 8

EXPLORE EPCOR MEMBERSHIP

EPCOR has membership opportunities for companies, businesses, corporations and Third-Parties.

Explore your options by calling 800.500.0100 or visiting www.epcor.org

EXPLORE EPCOR

Don't Let Faster Payments "Road-Runner" Over Your Organization!



Join us on
THE ROAD TO FASTER PAYMENTS!

- Four Learning Tracks Spanning Emerging and Traditional Payments
- National Experience at a Regional Price Tag
- Casual Food for Thought Discussion Forums
- Optional *How to Confidently Identify Third-Party Senders* Workshop
- Peer-to-Peer Networking
- Solution-Filled Exhibit Hall
- And More!

Spring Keynote: Jill Castilla, American Banker's Community Banker of the Year!

Register today in the online store at epcor.org.

EPCOR PAYMENTS CONFERENCE - SPRING 2018
HILTON COLUMBUS/POLARIS
COLUMBUS, OH
MAY 22 - 24, 2018

EPCOR PAYMENTS CONFERENCE - FALL 2018
SHERATON OVERLAND PARK HOTEL
OVERLAND PARK, KS
OCTOBER 24 - 26, 2018

epcor[®]

Electronic Payments Core of Knowledge

TOOLKIT continued from page 6

Addressing Common Misconceptions –

This promotional piece directly addresses and responds to common misconceptions about ACH payments, enabling nonprofits to offer factual responses to donors who may have questions.

“ACH payments are the gold standard for recurring payments, and nonprofits rely on recurring donations,” said Priscilla Holland, Senior Director, Healthcare & Industry Verticals, NACHA. “We designed the toolkit to help support the set up and promotion of direct withdrawal *via ACH* for sustaining donor programs that ultimately will help the nonprofits achieve their program goals.”



Research demonstrates that ACH payments can improve donor retention. According to early findings from a study commissioned by NACHA, donors who give *via ACH* donate more frequently than those who donate via other means. One major reason is because donors who use direct withdrawal *via ACH* can set up their donations to continue automatically until canceled by the donor.

CASH continued from page 7

Always be Consistent

When you're counting the money yourself, you need to do it the same way every time to avoid mistakes. Coins first and then bills going from lowest to highest denominations is one template.

Use a Deposit Template

Texas A&M University suggests a best practice for preparing a cash deposit. Only one currency per bundle with all the bills facing up. Don't use paperclips. A rubber band is the best way to hold bills together.

In addition to giving more often, direct withdrawal *via ACH* donors give more, donating more than double compared to donors who give via paper check, credit card or other means.

The research also shows that direct withdrawal *via ACH* is a payment method donors want to use. Donors cited “familiarity and comfort” and “quick and easy” as the most important factors when choosing their method of payment. Additionally, donors indicated that “the charity receives the donation quickly” and “the method is trustworthy” as additional factors when considering a donation method.

“Currently 82% of U.S. workers receive their pay *via ACH*—commonly known as Direct Deposit—and consumers pay more than 800 bills each month *via ACH*,” said Holland “Additionally, ACH payments are fast and easy. They can be set up online just as quickly as any other type of payment, and most payments can be received by an organization the next day. ACH transactions are safe and have the least incidence of fraud compared to other payment types. Clearly, ACH payments meet the needs and wants of donors.”

Source: NACHA.org

Keep Duties Separate

Checks and balances are important when your small business is handling lots of cash. The people who handle the money should be different than those responsible for bookkeeping.

Count in Private

Security is always a number one concern for a small business that owns vending machines. Only count money when you're away from the public or employees. If you store your cash in a safe, change the combination regularly.

Source: smallbiztrends.com

Older Americans Month 2018: Engage at Every Age

Across the country, older Americans—a rapidly growing population—are taking part in activities that promote wellness and social connection. They are sharing their wisdom and experience with future generations, and they are giving back to

Administration on Aging, OAM offers opportunity to hear from, support and celebrate our nation's elders. This year's OAM theme, "Engage at Every Age," emphasizes the importance of being active and involved, no matter where or when you are in life. You are

are engaging with friends and family, and through various community activities. Organizations can access free resources to conduct activities and share information in their communities.

The [CFPB's Office for Older Americans](#) has also provided tools to help people make better informed financial decisions to enhance their later-life financial security. They offer resources to help safeguard and protect older adults from financial exploitation. Support Older Americans month in May by using free resources developed to help older adults protect their money.

Here are a few ideas for your participation:

- Distribute the CFPB's [Managing Someone Else's Money](#) guides—brief, plain language information for financial caregivers.
- Use the [Administration on Aging's free posters](#) to foster awareness in your organization and in your community.
- Visit [consumerfinance.gov/olderamericans](#) or the [Administration on Aging](#) for more resources to share during Older Americans month.

And, join the Administration on Aging in celebrating by participating their Selfie Challenge! They want to see how you're engaging. Simply take a selfie (or have someone take your photo) and tweet it with the hashtag #OAM18. 📸



enrich their communities. They're working and volunteering, mentoring and learning, leading and engaging.

Every May, for 55 years, Older Americans Month (OAM) has been observed to recognize older Americans and their contributions to our communities. Led by the Administration for Community Living's

never too old (or too young) to participate in activities that can enrich your physical, mental and emotion well-being.

It is becoming more apparent that remaining socially engaged can improve the quality of life for older adults. Your organization can participate in OAM 2018 to focus on how older adults in your area



PEOPLES
NATIONAL BANK



Electronic Payments Core of Knowledge

EPCOR is your electronic payments core of knowledge and influence. We are a member-focused association devoted to providing personalized support and services.

The mission of EPCOR is to provide our members with the knowledge, support and industry representation necessary to succeed in the ever-evolving electronic payments business.



Through our direct membership in NACHA, EPCOR is a specially recognized and licensed provider of ACH education, publications and support.

© 2018, EPCOR. All rights reserved.

www.epcor.org

3100 Broadway Blvd., Ste. 555, Kansas City, MO 64111

800.500.0100 | 816.474.5630 | fax: 816.471.7665