Small Business Payments Toolkit

Business Payments Coalition | Volume 3 | 2017

TABLE OF CONTENTS

INTRODUCTION

This resource was created for small businesses and the bankers and advisors who serve them in order to encourage more efficient and safer payments processes by small businesses, as well as to provide education on payments fraud prevention. It is a project of the Business Payments Coalition (formerly the Remittance Coalition), a group of organizations and individuals volunteering to promote greater use of electronic business-to-business (B2B) payments and electronic remittance data exchanges. The team that produced this toolkit included bankers who serve small businesses, business practitioners, software and technology service providers, representatives from the Federal Reserve Banks, electronic payments networks and others.

This is the third volume of the Toolkit. Each volume builds upon the content released in previous volumes with new content and updates made to address the evolving nature of the payments system. This volume introduces new articles on Same Day ACH and on current payments fraud attacks. We added a Self Assessment Quiz to take after reading the Toolkit to determine how ready your small business is to start using electronic payments. We have also updated content throughout and included new links in the Resources section. To bring readers quickly to the content they are most interested in, the table of contents now allows you to click on a topic and be brought right to that page.

We hope you find the toolkit to be informative and helpful. As we work to create additional resources for you and make improvements to this toolkit, we welcome your feedback and thoughts. Please provide any insights to us by sending an email to business.payments.smb@mpls.frb.org

The Business Payments Coalition always welcomes new members and volunteers. To learn more, visit our website at: https://fedpaymentsimprovement.org/payments-efficiency/business-payments-coalition/

Note: These materials have been created by the Business Payments Coalition and are intended to be used as resources. Views expressed here are not necessarily those of, and should not be attributed to, any particular Business Payments Coalition participant or organization. They are not intended to provide business or legal advice, nor are they intended to promote or advocate a specific action, payment strategy or product. Readers should consult with their own business and legal advisors.

Business Check

A negotiable instrument (document) that instructs and authorizes the financial institution upon which it is drawn to pay a specific amount from the "drawer" (the signer or payor – the party making the payment) to the payee (the party receiving the check).

PROS:

Checks are a widely accepted payment method.

The check writer does not need to know the payee's bank routing number and account information..

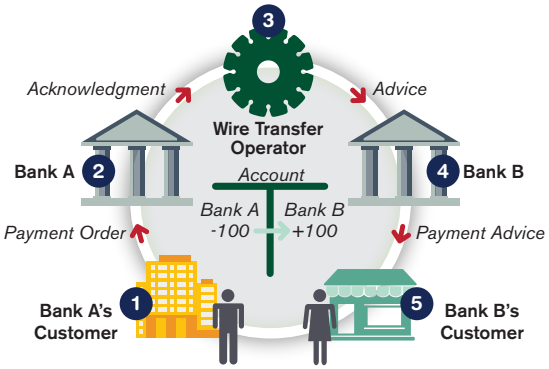
CONS:

Costs are high, including postage, purchase price of check stock, toner and labor of signing, stuffing and mailing.

Many people handle and see checks, so account numbers can be stolen/compromised, mail can be stolen and/or copies taken, creating the opportunity of fraud against the check writer's account.

Wire Transfer

The electronic transmittal of funds intra-day from one financial institution to another involving an unconditional order to pay a certain amount to a beneficiary upon receipt, or on a day stated in the order. Funds are irrevocable. Each wire transfer is a single message sent individually.



PROS:

A highly-secure, near-real-time mechanism that ensures domestic or international delivery and final settlement.

CONS:

Fees are charged to both the sender and recipient; fees for international wire transfers can be high.

The payor must know the payee's bank routing number and account information.

Credit and Debit Cards

Credit cards allow cardholders to make purchases or obtain cash advances using a line of credit granted by the issuer of the card. Credit cards allow cardholders to have a continuing balance of debt, subject to interest being charged.

Debit cards allow cardholders to make purchases or withdraw available cash from their own checking accounts.

PROS:

Accepting these payment types might boost sales; cards are easy to use and widely accepted; funds are secured/guaranteed from the cardholder.

The payor does not need to know the payee's bank routing number and account information.

CONS:

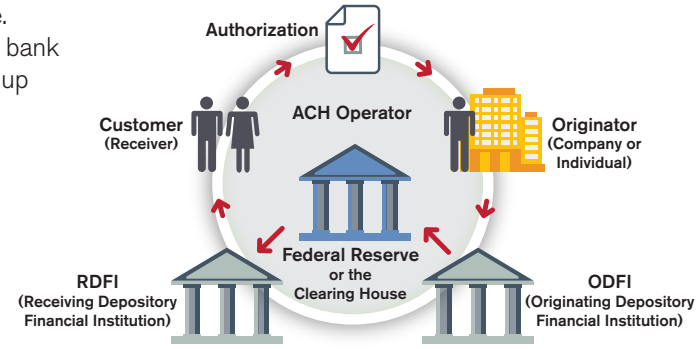
Potentially high cost of acceptance (monthly, equipment and interchange fees). Chargeback amounts and fees are incurred when a customer requests a reversal of a charge for reasons such as claiming fraud, dissatisfaction or non-receipt of service/product.

Automated Clearing House (ACH)

Electronic payment network that can be used to push (credit) or pull (debit) funds. Transactions are processed in batches (instead of as single items as in the case of a wire transfer or a check) with a one- or two-day settlement timeframe. Used for Direct Deposit of payroll, direct debit of recurring bills and various other use cases.

An ACH credit is an ACH entry originated to make a payment to another account; for example, from a buyer to pay a supplier for a purchase. The buyer's account is debited by the buyer's bank and the buyer's bank sends the payment to the ACH network. The supplier's bank picks up the payment from the ACH network and posts the credit to the supplier's bank account.

An ACH debit is an ACH entry that pulls a payment from another account; for example, used by a supplier to pull (debit) funds from the buyer's account for a purchase.



PROS:

ACH typically has lower fees per transaction than other types of payments described here. Transactions are typically seen by fewer people than check transactions (e.g., only the payroll or accounts receivable clerk might see an ACH transaction), reducing chance for fraud. In major disasters (e.g., Hurricane Katrina), ACH may process without delay, while paper checks may be more difficult to deliver and/or more easily lost. Employees and companies may receive payments faster when using ACH to send credits.

CONS:

Unlike wire transfers, which are irrevocable, ACH credit entries received are not final until settlement between banks takes place.

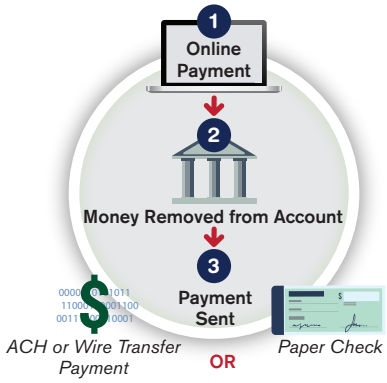
Recurring ACH payments are not guaranteed – the accounts on which they are drawn must have good funds in them.

The party originating the transaction must have the receiver's bank routing number, account number and authorization.

Internet Bill Pay

Internet bill pay is a type of electronic payment service that facilitates both one-time and recurring bill payments. It is a payment initiation service that relies on traditional payment vehicles like check and ACH to make the actual payment. Internet bill pay may be provided by either a financial institution or a non-bank provider. The provider sends an ACH payment or check on behalf of the bill payor. Electronic bill payment is commonly offered through a bank's online banking service, allowing a depositor to send money from his checking account to a creditor or vendor (such as a public utility) to be credited against a specific account.

Non-bank providers offer bill pay services for businesses. Electronic invoicing (e-invoicing) can be a very useful tool for the accounts payable department. It centralizes all transactional documents in one location on a web server so they can be easily found and processed. E-invoicing allows vendors to submit invoices over the internet and have those invoices automatically routed for processing.



PROS:

Saves time associated with paying bills. Can produce substantial cost savings compared to the traditional approach of printing and mailing bills and payment remittances. An added benefit is a significant reduction in the use of paper.

With e-invoicing, invoice arrival and presentation is almost immediate.

CONS:

If payment is made via check, checks mailed may take 5+ days to reach their destination. A check may have the payor's account number on the check, which can enable fraud. Depending on the bill pay service provider, checks for bill payments initiated may be outstanding until paid, so payors need to be aware of their true account balance.

The payor must know how to identify the payee to the bill pay system being used so the payment can be accurately delivered.

What Small Business Should Know About ACH

What is the ACH?

The Automated Clearing House (ACH) is a batch processing, electronic payment system that clears and settles most business payments in one day or two days. Same Day ACH is a new service that is being rolled out in phases. Virtually all types of ACH payments, including both credits and debits, will be eligible for same-day processing. Only international transactions (IATs) and high-value transactions above $25,000 will not be eligible. For more information on Same Day ACH, see page 11.

Here's how a business can use ACH:

- Business or organization or person sends payment instructions to its bank—e.g., an order to deposit payroll credits to employee accounts or pay a supplier or a bill
- The bank originating the ACH transaction groups similar kinds of payments received from multiple business customers into "batches" (e.g., payroll credits to employees or payments to suppliers) and transmits them in an electronic file to its ACH operator for editing and processing
- ACH operator electronically delivers payroll credits and supplier/bill payments to banks receiving payments on behalf of their customers (e.g., payroll deposit to employee or payment to supplier)
- The receiving bank credits the account of the receiver (e.g., employee or supplier)

Why is ACH Attractive for Small Businesses?

- It is secure and reliable
- ACH is especially useful for batch payments (e.g., payroll) and recurring payments (e.g., monthly bills like rent)
- After initial set-up cost, ongoing bank fees are relatively modest
- ACH allows for funding by checking or savings account, and/or pre-funding
- Fraud risk is lower than with checks; but business must monitor ACH debits received
- Remittance data (information that explains what the payment is for) can be included with the ACH item (in the addenda record)
- Acceptance is quite widespread among parties being paid

Things for Small Businesses to Keep in Mind When Considering ACH

- Initial set-up to originate or receive ACH may be technically challenging
- Originators of ACH payments must know banking account information (including routing/transit number and account number) of each business, organization or person who is receiving a payment
- Returns must be managed in a timely manner
- Rules and procedures are rather complex
- Although widely accepted, ACH payments are not as commonly accepted as checks
- Credit check/underwriting may be required for originators of ACH payments

When Does it Make Sense for Small Businesses to Use ACH?

Making payments:

- For payroll
- For recurring bill payments such as rent and utilities
- To pay taxes

Receiving payments:

- For businesses that bill recurring monthly payments such as child-care centers, property rental agencies, school tuition, service businesses and health clubs
- Health care – e.g., doctors, dentists (Federal government has mandated ACH for Medicare)
- Nonprofits that charge dues or fees or religious organizations that seek weekly or monthly donations
- To conduct business with entities that require electronic payments acceptance (e.g., some businesses and government entities)

What are the Main Benefits for Small Businesses Accepting ACH Payments?

- Increase business opportunities and build revenue:
  - Some large business and government entities will only do business with those who accept ACH payments
  - The Federal government is promoting electronic invoices and electronic bill payments with trading partners (see the website www.pay.gov)
  - Many younger generation consumers prefer electronic payments and processes
- Strengthen business retention: customers set up on recurring payments via ACH are less likely to change providers (e.g., gym, daycare, charitable donations)
- Reduce fraud: ACH payments are safer than checks
- Save money: reduce labor and administrative costs needed to process payments and remittance details
- Help manage cash flow: you can establish specific dates to make and receive ACH payments

Small Businesses Should Talk to Their Banks About ACH:

- Be proactive and contact banks about payment needs; don't expect your bankers to contact you
- Shop around; seek out banks with services that will help a small business who wants to become an ACH receiver and/or an ACH originator
- Seek out the ACH experts at your banks – e.g., ask small business, cash management or "treasury" experts for help (probably not loan officers)
- Bring information about your payments needs (payroll, examples and types of incoming and outgoing payments, etc.); don't settle for only online banking or a bill pay service
- Be prepared to complete complex authorization forms for risk underwriting and security
- Pursue risk management services offered by your bank:
  - Fraud/risk education
  - ACH debit blocks and filters

For more tips on communicating with banks, see "How to Talk to Your Bankers about Payments" starting on page 12 and "Bankers, Small Businesses and ACH: Getting on the Same Wavelength" starting on page 13.

Definitions of ACH Participants

An ACH payment and its related remittance data typically flows from 1) the ACH originator to 2) the Originating Depository Financial Institution (ODFI) to 3) the ACH operator to 4) the Receiving Depository Financial Institution (RDFI) to 5) the ACH receiver.

How the ACH Network Electronically Moves Money and Data

1. An individual, business or government agency initiates a Direct Deposit or Direct Payment transaction, such as payroll direct deposits, online bill payments or government benefits.

ACH entries are entered and transmitted electronically, making transactions **FASTER, EASIER, SAFER** and **MORE COST-EFFECTIVE** than paper checks.

UNIVERSAL

- The ACH Network connects virtually all 12,000 financial institutions in the U.S.
- Ubiquity allows consumers and businesses to confidently send and receive payments to one another.

2. The ODFI enters the ACH entry. The ODFI aggregates payments from all their customers, and sends them to the ACH Operator.

3. The two ACH Operators (the Federal Reserve Banks' FedACH® Services and the Clearing House's Electronic Payments Network (EPN)) receive batches of ACH entries from ODFIs around the country. All ACH transactions are sorted and sent.

EFFICIENT

- The ACH Network offers the unique ability to send meaningful data with payments for straight-through processing.
- The ACH Network provides businesses, government agencies and individuals a cost-effective way to make payments and get paid electronically.

SECURE

- ACH credit payments – like Direct Deposit – are one of the safest electronic payment types.
- ACH payments have a lower unauthorized return rate than credit cards and signature debit cards.

4. The RDFI receives the payment entry from the ACH Operator and applies it to the appropriate account.

5. An individual, business or other entity's account is debited or credited, according to the type of ACH entry. ACH payments are completed within 1-2 days.

INNOVATIVE

- The ACH Network has continuously evolved since its inception.
- Over the past 25 years, NACHA® has facilitated the adoption of 275 rules, creating new value for users.

Diagram created by NACHA and reprinted with permission.

EACH OF THESE PARTICIPANTS IS DEFINED BELOW.

ACH ORIGINATOR:

Business, organization or person who initiates ACH payment instructions.

- Usually a company, nonprofit or government entity; may also be an individual
- The ACH originator has a defined relationship with the receiver of the payment
- Initiates ACH payments based on valid authorizations from ACH receivers
- Responsible for securing and maintaining a copy of the authorization
- For business payments, has agreements with trading partners

ORIGINATING DEPOSITORY FINANCIAL INSTITUTION (ODFI):

Financial institution that initiates ACH payment file consistent with instructions received from its corporate (business) or consumer customer.

- Originator's financial institution receives payment instructions from the business/organization/person ("originator") that is originating these payments
- ODFI has an agreement with each originator (business, organization, person)
- Has exposure limits in place for each originator
- Transmits payment instructions into ACH network (to ACH operator)
- ODFIs may also receive ACH transactions – see Receiving Depository Financial Institution (RDFI) to the right

ACH OPERATOR:

An entity that clears and settles ACH payments between financial institutions (ODFI and RDFI).

- There are two ACH operators: The Federal Reserve Banks' FedACH® Services and the Clearing House's Electronic Payments Network (EPN); payments will travel over one or the other (and in some cases both)
- Serve as a central clearing facility for ACH payments
- Edit and process ACH entries according to rules developed by the National Automated Clearing House Association or NACHA—The Electronic Payments Association (see www.NACHA.org)
- Establish processing and exchange schedules for ACH network and deliver ACH payments to receiving point(s) according to published schedules
- Have agreements with each ODFI and RDFI outlining send/receive specifics

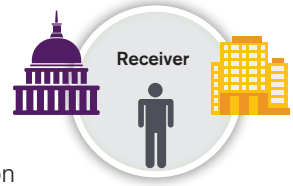
RECEIVING DEPOSITORY FINANCIAL INSTITUTION (RDFI):

Financial institution that receives the ACH payment file and applies payments to its corporate (business) or consumer customer accounts.

- Receiver's financial institution receives payment instructions (ACH transactions) from the "receiver" – the business, organization or person who is the account holder
- RDFI has agreement with each receiver (business, organization, person)
- RDFIs may also originate ACH transactions; that is, they may be ODFIs too

ACH RECEIVER:

Business, organization or person that receives the ACH payment.



- Receiving party to an ACH transaction may be a business, nonprofit, government entity or person
- Since the ACH receiver authorizes the originator to initiate the entry, the receiver must have a relationship with the originator
- The ACH receiver is an account holder at the RDFI

Consumer Versus Corporate Accounts

DID YOU KNOW?

ACH transactions are typically categorized as consumer or corporate
Depends on:

- The relationship of parties involved in the transaction
- The type of checking or savings account that receives the ACH debit or credit

Consumer or corporate accounts are governed by different rules
Pertaining to:

- How payments are authorized
- Return of funds options:
  - Time frame
  - Disputes

Consumer or corporate ACH transactions are identified by a transaction type code known as a standard entry class (SEC) code
Consumer codes:

- There are many consumer codes for both debit and credit entries:
  - Various ways to authorize
  - Timing for returns for non-authorized entries is governed by NACHA rules

There are only two corporate codes
Corporate codes:

- CCD: Cash Concentration or Disbursement (corporate credits or debits) may include payment remittance information (i.e., records have both funds and data)
- CTX: Corporate Trade Exchange will facilitate credits or debits and has multiple records of payment remittance information
  - Authorization is usually covered by contract or business billing relationship
  - Returns for non-authorized entries can be subject to short time frames. So check your account daily!

ACH Payments and Remittance Solutions

What You Need to Do to Pay via ACH Using an Electronic Data Interchange (EDI) Remittance Format

Details associated with a paper check remittance should be included in whatever electronic format is agreed upon between the buyer and the seller. Examine the payment detail to be sure it matches the overall payment amount.

Critical Data Points Needed for Each Electronic Payment:

- Payer company name and banking information (routing/transit number and account number)
- Payment reference number:
  - Similar to a check number, this helps the buyer and seller identify a specific payment if questions arise
- Good funds date:
  - Critical to ensure the bank processes the payment timely and needed by the buyer to determine if cash discounts are available
- Buyer name and banking information (routing/transit number and account number)
- Invoice number, date and amount(s)[1]
- Cash discount taken (if applicable)
- Deduction reference number(s) and amount(s):
  - If available, include the deduction reason and details

Key Questions to Ask before Starting to Pay Electronically:

- How many billers will let me pay electronically with an ACH and EDI remittance format? This is critical because you may receive improved terms of sale by paying electronically, which could offset any start-up costs.
- Is my company EDI capable? If the answer is "yes," review the biller's technical requirements with your information technology (IT) group (or IT provider). If the answer is "no," examine alternative solutions with your bank or a third party.
- What do I need to ask my bank or a third party?
  - If you can send a file of remittance data to your bank, can the bank translate it to EDI for you (i.e., can the bank initiate the EDI remittance)? Make sure you agree on the format needed. Note: Your usual branch banking representative may not be able to assist you with this review. If not, treasury management or product management from your bank's corporate office may need to help determine the bank's ability to meet the biller's requirements.
  - If your bank cannot support the data conversion, you will need to talk to a third party.
  - If you can't send a file of remittance data, does your bank or third party have a portal where you can manually input payment details? Will the output of that entry meet the technical requirements of the biller? Can your bank or third party handle sending this remittance information with the ACH payment?
  - Whether using a bank or a third party, make sure you send a test file of remittance information with a nominal monetary ACH payment to the biller for review.
  - Make sure your bank or third party has an EDI translator to accomplish the task of configuring your data into an EDI-compatible format.
- *Is this cost effective for my company?* Talk to your finance or treasury advisor to do a cost benefit analysis. Your bank may also be able to assist.

[1] Use relevant sales document (e.g., contract, purchase order) if customer does not pay off of buyer's invoice.

Same Day ACH: An Important New Payments Tool for Small Businesses

What's it all about?

One of the major changes to hit the U.S. Automated Clearing House (ACH) network in years is the ability to send Same Day ACH items. Prior to this new capability, most ACH payments were settled one or two business days following transmission. For example, if you sent a payment to a trading partner on Monday, it typically would get there Tuesday or Wednesday based on the type of payment. With Same Day ACH (which is being rolled out in phases), depending on your bank's capabilities and when you send the payment, a payment can get to your trading partner's bank by the close of business on the same day.

Wondering why would you use it?

Suppose your company sends a payroll for processing but due to a processing error funds cannot be delivered to your employees in time to meet the effective payroll date. With Same Day ACH you can expedite the payroll and employees will get paid today. Another application is to pay temporary employees who must be paid at the end of each week. Or, perhaps you need to make a vendor or tax payment today to avoid a late fee. Same Day ACH offers a solution to these situations.

Examples of payments you can make with Same Day ACH include person-to-person payments, mortgage payments, tax payments, bill payments, invoice payments, account transfers and insurance refunds.

The way Same Day ACH works, all receiving financial institutions in the U.S. must accept these payments so you don't have to worry about the receiving bank not participating or your client not receiving the payment. As long as your bank allows you to make a Same Day ACH payment, the receiving bank will receive and post the payment to the specified account.

RULES OF THE ROAD: THREE PHASES

Same Day ACH supports all payment types except International ACH Payments (IAT). It is being implemented in three phases. The phases pertain to whether the payments are credit or debit payments and the timing for funds availability.

PHASE 1: (AS OF SEPTEMBER 23, 2016)

With this first phase of Same Day ACH the rules are:

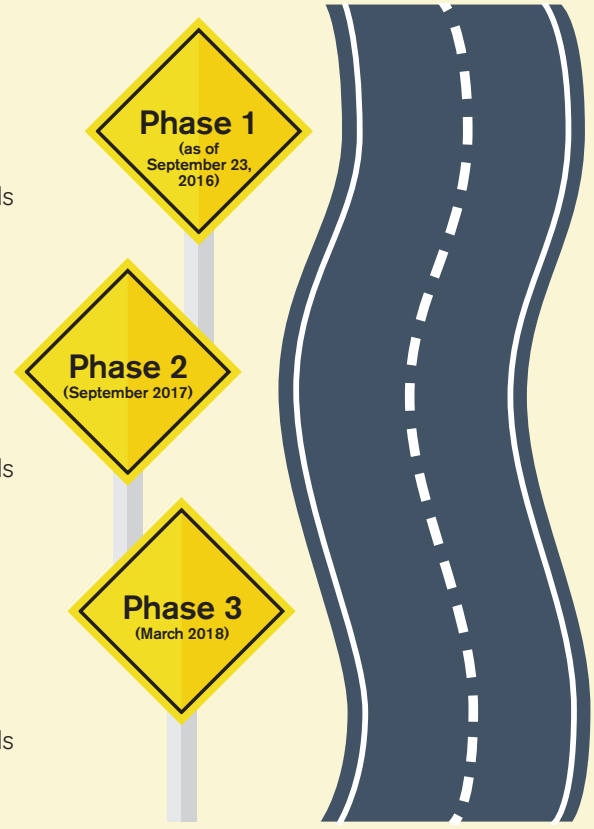
- Credit payments only
- $25,000 limit per item
- Funds availability: the receiving bank has to make the funds available to the receiver's account by the bank's end of processing day (local time)

PHASE 2: (SEPTEMBER 2017)

- Credit and debit payments
- $25,000 limit per item
- Funds availability: the receiving bank has to make the funds available to the receiver's account by the bank's end of processing day (local time)

PHASE 3: (MARCH 2018)

- Credits and debits
- $25,000 limit per item
- Funds availability: the receiving bank has to make the funds available to the receiver's account by 5:00 p.m. local time



How to Talk to Your Bankers About Payments

1. Establish a relationship with a financial institution (bank or credit union)

Seek out financial institutions that offer:

- Small business-focused online banking with robust bill presentment and payment services
- Services to set up small businesses as ACH receiver and originator
- Card solutions (e.g., purchasing cards, credit and debit card acceptance)
- Remote deposit capture (RDC) (allows a business to scan checks and transmit the images to a bank for posting and clearing).
- Prepaid payroll cards, if desired
- Fraud monitoring and prevention tools, including alerts
- Merchant services, if necessary

2. Talk to your banker about your payments needs

As a small business, you must be proactive about contacting your bank(s) about your payment needs; don't necessarily expect your bank(s) to contact you. Seek out a small business expert at your bank. Bring information with you about your payment needs (payroll, incoming and outgoing payments, card usage, etc.). Also ask your banker about free and priced risk mitigation services offered by the bank, such as fraud/risk education, ACH debit blocks and filters and fraud and risk alerts. For more, see ACH Fraud starting on page 22.

Be sure to talk to your banker about these payment options:

- Using online bill pay
- Using RDC and/or mobile RDC
- Using ACH. This will allow you to pay employees via Direct Deposit. Being set up as an ACH Originator will likely require underwriting, which will allow the bank to establish an exposure limit for your organization.
- Accepting payments via credit or debit cards. Your business banker may be able to help you establish a merchant services account. In addition to, or instead of, traditional card acceptance, you may want to use a device (such as Square®, PayPal Here® or Intuit® GoPayment®) which attaches to your cell phone, allowing you to turn your smart phone into a card acceptance device.

3. Talk to your banker about pricing

Fees for payment services may vary greatly by bank and may be negotiable. Fees you might encounter while setting up services with your bank include initial set-up fee; ongoing fees like monthly service fees; transactional fees such as per-batch, per-item, reject and notification of change (NOC) fees; and others, such as fees associated with cash management reports.

4. Whenever possible, try to send and receive payments electronically

Electronic payments are generally faster than checks. As the U.S. Postal Service® continues to close processing centers throughout the country, the time it takes for a piece of first- class mail to arrive at its destination will continue to increase.

Many payments experts consider electronic payments to be generally safer than checks or cash. According to research, checks are the primary target for fraud attacks at businesses.[2] Electronic payments sent directly from and to your account are much less likely to be compromised than paper checks. For more on Check Fraud, go to page 21.

Electronic payments are generally less expensive than relying on business checking accounts.

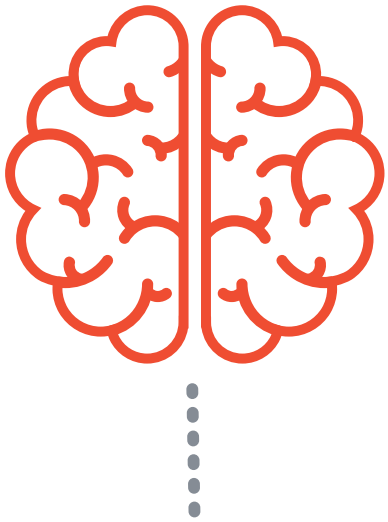
[2] 2016 Association for Financial Professionals Payments Fraud and Control Survey, Report of Results, March 2016.

Bankers, Small Businesses and ACH: Getting on the Same Wavelength

As a small business, it is important for you to have in-depth discussions with your banker about your payments goals. To help prepare you for these discussions, review the following preconceptions some bankers may have and consider some suggestions to ensure a productive conversation. The more you're able to overcome potential conversation barriers, the better equipped you'll be to achieve your payments objectives.

Preconceptions Some Bankers May Have about Small Businesses and ACH

- Small businesses may not generally be knowledgeable about ACH – including subtleties like the difference between an ACH debit vs. an ACH credit
- Small businesses may not distinguish between "wires," "Direct Deposit," "EFT," "electronic payment" and "ACH," using these terms interchangeably
- It may be hard for small businesses to rationalize monthly costs: there may be a misalignment between small business payments volume and ACH fees. How many ACH payments are needed to justify costs?
- Small businesses may be unfamiliar with, or intimidated by, the electronic payments questions posed to them
- The underwriting (credit approval) process required to originate ACH items may be tedious for small businesses (there may be many forms to fill out)
- Small business may be intimidated by annual ACH audit requirements
- Managing the payment identity of payees may be challenging for small businesses (payment identity refers to the payee's bank account routing/transit number and his/her checking account number)
- Small businesses' ACH origination, receipt and reconciliation are most likely not integrated into their current payment processes
- Checks may be easier for small businesses to manage than ACH



Suggestions and Tips: Talking to Your Banker about ACH

Given these potential preconceptions, consider the following suggestions and tips when entering into discussions with your banker:

- Remind your banker that since many small businesses may be aware of electronic payments for payroll, banks should leverage what small businesses already know about ACH
- Ask for a specialized bank staff person and materials that explain/educate about ACH, if needed
- Ask your bank to explain security costs
- Ask for your banker to explain how many ACH payments you will need to make to justify costs
- Ask for details on the comparative fraud risk of checks vs. ACH
- Find out about ACH fraud prevention tools and alerts offered by your bank
- Ask about options for your bank to bundle costs into base fees and offer incentives; ask if ACH services can be bundled into base fees for online banking
- Ask your banker if they provide consulting services to help you set up ACH origination and simplify ACH credit origination for all businesses – they may direct you to an integration service provider
- Ask about your options to make ACH available automatically on all or selected new accounts
- Ask about the revenue gain opportunities for your business via account analysis reports
- Ask about the workflow and control issues you may need to address; for example, segregation of duties is a recommended best practice to implement ACH
- Ask about the need to manage and secure the payment identity of each payee, including the payee's routing/transit number and his/her checking account number:
  - How should a small business obtain this information?
  - Where should this sensitive information be stored?
  - How should updates and maintenance be handled?

Tips on Getting Started Originating ACH

While there are different ways to create (originate) an ACH transaction, the two most popular methods include:

1. Working through your bank's online banking system

This means entering your transactions directly into your bank's online banking system.

PROS:

This can be very appealing for originating low volumes of ACH transactions, and can minimize the time involved for setup and ongoing maintenance.

CONS:

Originating ACH transactions through your banks' online system can be labor-intensive, requiring manual entry of each transaction into your bank's online system or when adding payment templates. Also, it may not allow for ACH debits (i.e., collections from customers). In addition, any process that involves re-keying of data can be error-prone.

2. Creating an ACH file yourself using ACH file creation software

Creating an ACH file in-house may be an ideal option if you want to use information from your accounting package, an online store, a database or even a spreadsheet. An ACH file is a specially-formatted file that contains ACH debit and credit instructions for your bank, referred to as a NACHA file.

PROS:

If you create an ACH file in-house, you can create transactions without manually re-keying your data, increase security by splitting responsibilities and review (segregation of duties), and handle any type of ACH transaction (SEC – Standard Entry Class). Thus, it may be more flexible than originating ACH transactions via a bank's online banking system.

CONS:

This method may require a little more time for setup, and may require additional expense to hire a third-party program to help you create the ACH file.

Frequently asked questions about ACH file creation:

Can my accounting package create an ACH File?

Unfortunately, not all accounting packages have the ability to create an ACH file. While many accounting packages offer electronic bill pay and direct deposit capabilities in which the data is processed by the accounting software's own processor, this scenario may not enable you to create an ACH file and originate it directly through your bank. What's more, utilizing this service would typically cost more – per transaction – than processing with your bank.

What about QuickBooks®?

While QuickBooks cannot create an ACH file, there are a number of third-party add-ons that give you this capability. While we cannot recommend any specific add-ons, you can find a number of third-party add-ons via an internet search (i.e., "QuickBooks ACH File")[3].

My accounting package can't create an ACH file. Can I create one without using software?

While the ACH file format is publicly available (i.e., search for "ACH File format"), it is recommended that you use a tool to help create the file as these utilities not only format the file, but also follow certain batching (grouping) rules, create summary and hash totals, and follow specifications of NACHA—The Electronic Payments Association, the rule-making body for the ACH system.

Some bank payment systems can accept other formats (e.g., csx, .txt) so check with your bank to see what other payment file formats may be available.

[3] We have addressed QuickBooks here as QuickBooks has a significant market share in the small business community.

How Should I Evaluate ACH File Creation Software?

There are many factors to consider when selecting software of any kind – including functionality, pricing, vendor reputation/credentials, support policy, update schedule, training/implementation, scalability and ease of use – just to name a few. The following guidelines focus on ACH functionality.

ESSENTIALS

1. Does the ACH software create an ACH file in the SEC code you need?

Prearranged Payment or Debit (PPD) and Cash Concentration or Disbursement (CCD) are the most commonly requested SEC codes by small business users – and the majority of ACH software packages will create them. If you need other codes, such as Corporate Trade Exchange (CTX), you should confirm that your software package can create the EDI[4] detail. If you need Telephone-Initiated Entry (TEL), Internet-Initiated Entry (WEB), International ACH Transaction (IAT) or any other SEC code – confirm with the vendor that these can be accommodated.

2. Does the software handle pre-notes, offset records and addenda records?

While these are all basic functions, vendors handle them all very differently. Don't rely on a specifications sheet; make sure you test (see number four below). Also, be sure that your software can initiate both debit and credit pre-notes. A pre-note, which is short for pre-notification or pre-authorization, is a zero dollar transaction created and sent through the ACH network to test the validity of the bank transit/routing number and the payor's/payee's bank account number.

3. Are you able to integrate the software with your data – whether an accounting package or simply a spreadsheet?

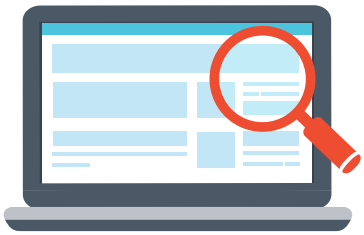
An important consideration for many people is to ensure that they are able to import data without manually keying it in. For example, packages like QuickBooks allow you to pull transactions directly from your data files so you do not need to export or import files.

TEST, TEST AND THEN RETEST

4. Is there a free download available for your test?

With the ACH software, you should be able to create an ACH file with your data and send it to your bank to confirm. Your bank may offer multiple file templates that adjust your file format for downloading to their system.

5. Is it easy to use?



Ask yourself, "Is this a program I can use?" and "Is it easy enough for someone else in my department or at my business to create an ACH file when I'm out of the office?" Also, take a look at the user help files and documentation. Introductory training videos can also be helpful.

SUPPORT

6. Is phone support available – and what kind of assistance do they provide?

Will the software company help you set up the program? Are they knowledgeable about ACH/NACHA issues? It is always a good idea to call the software vendor before licensing – to see if you get through. If you can't reach a person during the pre-sales/sales process, it may be a warning sign that you'll be unable to reach them when you want support later on.

POPULAR ACH SOFTWARE FEATURES

7. Can you email remittance "check stub" information to your vendors?

You should be able to send an email with detailed check stub information indicating the invoices and related amounts that you have paid via ACH.

8. Can you easily create a reversing entry if you make a mistake?

If you make a mistake, is there an easy method ("Point and Click") in place to let you reverse an ACH transaction that has already been sent to the bank? (Check with your bank for situations where a reversal is allowed.)

9. Can the process be automated?

Can the entire process be automated, from data import to ACH file creation to file transmission?

10. What security is in place? Is encryption available?

At a minimum, you should be able to password-protect user access, and there should be a full audit trail for each transaction (from import to ACH file creation). Ask if the internal data files can be encrypted ("data at rest") with Advanced Encryption Standard 256 Bit Encryption (AES-256), and if applicable, if the ACH file transmission process can be encrypted ("data in transit") with Secure SHell File Transfer Protocol (SSH-FTP).

[4] Electronic Data Interchange (EDI) is the computer-to-computer exchange of business documents in a standard electronic format between business partners. To get an overview, visit: www.edibasics.com/what-is-edi/

LICENSING

11. Can the software be installed on more than one computer for the purpose of disaster recovery?

The ACH software license should cover multiple machines for uninterrupted access for disaster recovery purposes. In addition, ask if there is an automated backup process available for the data files.

12. Does the software license cover both debit and credit transactions?

Most licenses cover both debits and credits, but some do not. Check carefully.

13. Do I have the option of either subscription or traditional licensing?

While there are advantages to each, if you opt for subscription licensing, make sure that it can be canceled at any time without penalty.

Subscription licensing pros:
Monthly payments let you avoid the upfront financial burden of purchasing software. In addition, it makes the software company "earn" its value each month as it typically includes software updates (both IT and NACHA), as well as client support.

Traditional licensing pros:
For businesses with a longer-term financial horizon, this may be more cost effective over time. Be sure to inquire about maintenance contracts so you'll have access to ongoing support and updates.

FUTURE GROWTH

14. What is the company's update policy?

- How often are updates posted?
- Are they simply IT/security updates, or do they include ACH rules (NACHA) updates?
- Are you able to view a version history of the software updates?

15. Same Day ACH is coming – does the vendor support it?

What are the vendor's plans for Same Day ACH?[5]

16. Can the system handle multiple origination accounts in the same ACH file?

Can the software handle transactions originating from multiple bank accounts in your organization, such as a payroll and a disbursement account?

17. Can the software re-submit transactions from an ACH Return File?

Not all ACH transactions are successfully completed. For example, debit transactions (i.e., collections from customers) can be returned due to insufficient funds. How your bank notifies you of these failed items can vary. One method is to send you an ACH Return File. Can the ACH software utilize this file and enable you to resubmit certain transactions?

18. Is it scalable? Will you outgrow the software?

- Does the software vendor support multi-user platforms with a central database?
- Is there a segregation of duties feature which enables you to grant/restrict feature access on a per-user basis?
- Can the software be used in a remote desktop environment? Can it operate in either a stand-alone or clustered environment?
- Is it compatible with different operating systems?

[5] Learn more about Same Day ACH at this site: www.frbservices.org/resourcecenter/sameday_ach/index.html or watch the video "Same Day ACH: How Will You Benefit?" at www.youtube.com/watch?v=K_XsiQ_54B0 Also, check out NACHA's Same Day ACH Resource Center: https://resourcecenter.nacha.org/

Additional Things to Consider When Evaluating ACH File Creation Software

Are there any features that you might need in the future? If you change your accounting package in the future, would you lose certain capabilities?

Think about features you might need in the future as your accounting and internal systems change. For example, does the ACH software have the ability to create profiles for customers, employees and vendors? Can the ACH software warehouse records (place on hold, then release), or create recurring transactions? Check to see if the software has the capability to convert ACH files to Excel®/CSV (useful for passing data to additional systems) and merge ACH files.

Other Payment Related Services

Does the vendor support positive pay issuance file creation to prevent posting of fraudulent transactions?

Positive Pay and Payee Positive Pay are bank-offered anti-fraud programs to help protect against altered and counterfeited checks clearing your account. To obtain this protection, entities send their bank a list of checks that they've issued. Subsequently, when a check is presented against the account, the bank compares the check information on the check against the information on file (from the list of checks sent by the client). If the check information matches, the check is cleared. However, if there is a discrepancy, the check will be placed on hold, and the bank will ask the client to make a "pay" or "no pay" decision.

While check positive pay services are generally more common, many banks offer ACH Positive Pay or ACH Payee Positive Pay services which are designed to ensure that only authorized ACH transactions post to your bank account.

The format of the issued transaction (check or ACH) file that the client sends to its bank varies by bank, and many larger banks have multiple formats. If this is or eventually may be one of your treasury management needs, ask whether the software vendor supports positive pay issuance file creation.

Does the vendor provide a reconciliation feature?

While virtually all accounting packages provide some level of reconciliation features, many accounting packages in the small business marketplace do not have the capability to handle data originated outside of their system. As many ACH transactions originate outside of the accounting system – notably user initiated transactions in online stores, or core business systems (membership/recurring billing, insurance premiums) – these activities may need the support of a reconciliation function.

ACH Returns and Notifications of Change (NOCs)

ACH electronic entries (payments) are categorized as "consumer" (subject to Regulation E) or "corporate/business" (subject to UCC 4A) for applicable return rules. For your protection, when either initiating or receiving an ACH item, it is useful to have an understanding of the difference between these two categories. The main difference is that consumer returns may be returned within 60 days of posting to the consumer's bank account, but corporate/business returns submitted after 24 hours of receipt must be first approved by the Originating Depository Financial Institution (ODFI). Classification of "consumer" vs. "corporate" is determined by account ownership.

Returns of ACH Items Originated by Your Business

- If you are using a business account, your financial institution (FI) will notify you of a return and then credit or debit the amount to your account to reflect the nature of the return. Return notification is typically provided to you by regular mail, email or online notification.
  - If you have questions concerning your responsibility in regard to the returns process, contact your financial institution.
- The only transactions that can be re-presented for settlement are (1) those returned for Insufficient Funds or Uncollected Funds (there is a limit of two re-presentments), or (2) a transaction that was returned for Stop Payment (if re-presenting it was approved by the receiving party.)
- A return may be initiated because the financial institution was unable to locate the account number, which means the FI was unable to identify the information as provided in the original transaction, so it could not be posted.
  - If this happens, the party intended to receive the transaction has no knowledge that the item tried to post and the Originator will need to contact the receiver to obtain updated information (e.g., account number and/or routing number) so a new transaction can be initiated.
  - It's also possible your customer changed bank accounts and simply forgot to notify you.

Returns of ACH Items Received by Your Business

It is imperative that every business check all bank accounts daily in order to be able to request the return of an unwanted transaction in a timely manner, in accordance with the return window for the account. As noted above, once an ACH item has posted to a business account, the business has only 24 hours to return an ACH item. After that 24-hour window expires, a business must obtain the approval of the ODFI before returning an item or settle the payment outside of the network.

NOTIFICATIONS OF CHANGE (NOCs)

If the information on a transaction you originated is incorrect, you may receive a non-dollar correction transaction called a Notification of Change (NOC). It specifies information such as:

✓ Correct account number

✓ Correct routing/transit number

✓ Correct account type (checking/savings etc.)

For example, if a receiving bank (also called Receiving Depository Financial Institution or RDFI) has been through a merger, it may send you a NOC to provide new information that should be included on future transactions that you originate.

Your financial institution will notify you of any NOCs received. Changes need to be made before originating future transactions. This is important to avoid disruption of payments or fines for uncorrected information which your financial institution may pass on to you. By following the NOC process, the receiving bank ensures that the information provided on future ACH transactions will be correct. By complying with the NOC, your business can originate future transactions without having to obtain a new authorization.

Tip: The following link will take you to the Federal Reserve Bank's website where you may search for valid routing numbers: www.frbservices.org/operations/epayments/epayments.html

Differences Between Consumer and Business ACH Returns

Consumer	Corporate/Business
When the consumer sends a return to their Receiving Depository Financial Institution (RDFI), the FI must process the return within 24 hours	When the business sends a return to their Receiving Depository Financial Institution (RDFI), the FI must process the return within 24 hours
EXCEPTION: Unauthorized transactions may be returned within 60 days of posting to the consumer's account	Returns beyond 24 hours MUST be approved by the Originating Depository Financial Institution (ODFI)

"Can I Pay You by ACH?"

Sample Trading Partner Agreement to Start Receiving ACH Payments

Do you have a customer who wants to pay you using ACH payments? Are you courting a potential new customer who pays through ACH exclusively? If yes, they may approach you with a trading partner agreement similar to the one shown to the right.

A word about terminology: some people use the term "EFT" (electronic funds transfer) interchangeably with ACH payments. However, the more specific term "ACH" is preferable. ACH refers only to automated clearinghouse payments, but EFT can refer to ACH or wire transfers.[6]

The trading partner agreement shown on the right is meant to give you an idea of the type of document you will be asked to complete and sign in order to set up your customer to pay you using ACH. The actual agreement you will be presented with will likely look different from this one, as there are many forms used in the market. In most cases, the customer will ask to send an ACH credit payment to the bank account you specify. Another approach, used less often and generally by those trading partners with a long-standing relationship, is to set up an agreement whereby the seller initiates an ACH debit entry to remove funds from a customer's bank account at a specified time with an agreed-upon amount.

Once you receive the trading partner agreement, read through it carefully. Follow up with the trading partner if you have any questions. Seek advice from your legal counsel, banker(s), accountant and other trusted advisors before you complete and submit the form. Keep the signed agreement on file.

Your banker can answer questions about how ACH works. Also, look on pages 6-11 of this Small Business Payments Toolkit for basic information about ACH. In addition, every part of the United States is served by regional payment associations (RPAs) who can offer advice and knowledgeable resources on ACH. If you are new to ACH and want more information about the ACH network before you agree to be paid via an ACH payment, refer to the list on page 44 in the Resources section and contact your local RPA to get your questions answered.

SAMPLE TRADING PARTNER AGREEMENT

VENDOR INFORMATION: **ABC Accounts Payable Vendor Number**
_____**(BY ABC)**

Vendor Name: _____ Vendor Taxpayer ID #_____

Accounts Receivable CONTACT: **CORRESPONDENCE ADDRESS:**
Name: _____ Address: _____
Phone: _____ City: _____
Email: _____ State: _____Zip Code: _____

VENDOR BANK INFORMATION:
Bank Name: _____
Address: _____
City: _____ State: _____ Zip Code: _____
Bank Contact Name: _____
Bank Contact Phone: _____
Bank ABA# or Routing # (Must be 9 digits): _____
Bank Account Number: _____
Name on Account: _____

Complete the following section only if you will use Electronic Data Interchange [EDI] for remittance information:
REMITTANCE INFORMATION:
_____ EDI Option – EFT Bundled (payment remittance sent within the 820 to your bank)
_____ EDI Option - 820 to your Value Added Network [VAN] or third-party EDI provider
_____ Non-EDI Option – Email Email Address: _____
Non-EDI Remittance must be received by VENDOR no later than: _____

EDI CONTACT (if applicable):
Name: _____
Phone: _____
Email: _____

NEW PAYMENT TERMS EFFECTIVE WITH SWITCH TO Automated Clearinghouse [ACH]:
_____

AGREEMENT:

1) VENDOR authorizes ABC to initiate ___credit or ___debit entries (check one) to the bank account noted above.
2) Prior to submitting its first electronic payment, ABC will perform an ACH test of $0.01 in order to verify connectivity between ABC and VENDOR banks. In ACH terminology, this small live payment is referred to as a "prenote" or "penny test."
3) VENDOR agrees that obligations with weekend or holiday due dates (banks closed) will be due for payment on the next business day.
4) VENDOR may change its designation of bank or bank account by written notice to ABC. Notice must be received by ABC's contact at least thirty (30) days before the effective date of the change or termination.

This agreement is effective on the date the last party hereto signs.

_____ _____ _____ _____
Vendor Authorized Signatory Date ABC A/P Director Date

[6] Refer to pages 4-5 of this Small Business Payments Toolkit for definitions of these payment types.

What Kind of Checking Account Should I Have for My Small Business?

When considering whether to open a personal or business account for your small business, www.sba.gov suggests that a business account:

- Keeps your books in order
- Gives your business a professional image

A Business Checking Account:

- May help you manage your cash flow
- May build your business brand with your company name on a check/debit card: customers will be paying a "company" not an individual
- May be easier and less costly than using a personal checking account from an accounting perspective as your business grows

Other Potential Outcomes From Having a Business Checking Account

Qualify for Business Credit Card	• Expense reporting may be easier • Can be used as a line of credit with rewards/perks
Ability to Utilize Business Banking Products	• Set-up merchant account to accept credit cards • Utilize ACH for payments and collections
Opportunity to Build Relationships	• Businesses benefit from a relationship with an accountant, an attorney and a banker • Business bankers can help – ask to meet with one when opening the business account

The Following Best Practices and Tips May Help Small Businesses Combat Payment-Related Fraud. All Payment Methods Carry the Risk of Fraud.

Check Fraud

Common types of check fraud include:

- Mail theft (after which a check is typically altered and presented for deposit or for cash)
- Counterfeit checks (printed/endorsed)
- Duplicate deposits (e.g., an item deposited via mobile remote deposit capture at a financial institution might be taken to a check-cashing facility or other financial institution and cashed)

Precautions you can take to protect your business from check fraud:

- Implement strong internal controls and procedures around accounts receivable (A/R) and accounts payable (A/P) functions
  - Reconcile your bank accounts daily
  - Address exception items and make timely returns
  - Apply separation of duties within the organization when it comes to checks; for example, no one person should be able to complete the check issuing process — access check stock, issue the check and reconcile the account — from start to finish
  - Secure blank check stock, deposit slips, canceled checks and statements
  - Manage control of checks from printing (if printing in-house) through mailing
  - Use secure financial document destruction processes, such as shredding old documents
- Leverage tools and processes available from your bank and reputable service providers; enact best practices in A/R and A/P functions
  - Whenever possible, make payments electronically
  - Use positive pay, reverse positive pay or positive pay with payee verification (See the box on page 17 for a definition of positive pay and payee positive pay)
  - Apply post-no-checks restrictions on depository accounts
  - Use point-of-sale (POS) check fraud detection services; e.g., shared database with rules-based systems and scoring
  - Require signature verification
- Educate and train employees on check fraud prevention
- Consider whether your small business even needs to accept checks as payment. To avoid potential losses due to check fraud, some merchants no longer take checks.
- Limit the number of checks issued
  - Replace employee paychecks with electronic payment options (Direct Deposit or payroll cards)
  - Consider outsourcing check writing to your bank so you no longer have to keep check supplies around

ACH Fraud

Common types of ACH fraud include:

- Unauthorized debits to your account
- Check positive pay rejects represented as ACH debits
- Origination of fraudulent items by an insider
- Email scams (e.g., phishing, "spear phishing") that allow the hacker to take over a computer and generate a bogus file
- Corporate account takeovers, through which hackers originate fraudulent ACH payments
- Fraudulent claims of unauthorized debits in accounts receivable

Precautions you can take to protect your business from ACH fraud:

ACH Debits

Tips to help avoid fraud losses associated with ACH debits:

- Limit ACH debit activity to a small number of accounts
- Reconcile your bank accounts daily and notify your bank of any suspicious transactions
- Address exception items and make timely returns
- Use fraud prevention services offered by your bank
  - ACH blocks on all accounts where ACH debit activity will not be used
  - ACH filters, which let you establish criteria that your bank will use to post or return ACH transactions
  - ACH positive pay or payee positive pay
  - ACH debit alerts that notify you when ACH debits post to an account
  - A recommended best practice is to block ACH debits on all accounts except on a single account that is set up with an ACH debit filter and/or ACH positive pay
- Secure your bank account information; lock up paper documents and limit access to sensitive online data
- Restrict access to any computer used for ACH transactions; don't allow web surfing, online shopping, social media access or personal email usage on that computer
- Use strong passwords and change them often
- Use an out-of-band authentication process when files are originated

ACH Credits

Tips to help avoid fraud losses associated with ACH credits:

- Implement best practices for online and IT data security, such as:
  - Adopt stronger form(s) of authentication or added layers of security
  - Dedicate a PC for ACH origination
  - Use logical and physical controls for payment processing
- Use dual controls for payment origination and account set-up
- Implement proactive detection and monitoring. Check if your bank offers these services:
  - Single item authorization
  - Notice of new payee added
  - Transaction, batch or file limits
- Develop and use files of known fraudulent recipients
- Require due diligence of third-party processors
- Educate employees on fraud and prevention

Mobile Banking Fraud

Using a smart phone or other mobile device, such as a tablet or laptop computer, to access mobile banking applications is convenient and saves time. However, be aware of the risks of mobile banking and become knowledgeable about measures you can consider taking to protect your small business from payments fraud attacks made over mobile banking channels.

Potential Risks of Mobile Banking

- Privacy and integrity of business banking data on or accessed through a mobile device may be compromised
- Malware and viruses may infect business banking data on or accessed through a mobile device
- It may be difficult to authenticate and authorize business mobile users accurately and securely

What You Can Do to Mitigate Mobile Risks

- Use encryption and strong passwords on mobile devices
- Disable wireless, Bluetooth® and Near Field Communication (NFC) when not in use
- Properly configure and patch operating system and software programs
- Regularly update firewalls, anti-virus and anti-spyware programs
- Limit access to business systems and data based on need to know
- Develop and follow cyber security polices specific to your business; require violations to be reported to management

Purchasing Card Fraud Prevention

Purchasing-card (P-card) fraud prevention tools to consider include implementing up-front controls, conducting regular compliance monitoring and investing in education and training.

Use P-card program tools and controls offered by the card issuer

- Block unauthorized vendors
- Use online services to view activity
- Limit the use of the card to specific merchant category codes (MCCs; also known as merchant classification codes). This way you can prevent charges at liquor stores, movie theaters, cash advances, etc.
- Place limits on the dollar amounts of transactions and the velocity with which transactions can be made (e.g., per day, week, month)
- Segregate administration, approval, auditing and reconciliation duties among different staff members

Monitor transaction activity

- If your transaction volume warrants it, request Level III data from P-card issuer[7]
- Require managers to review purchasing activity of subordinates
- Conduct spot or random audit of receipts. For example, one corporate treasury vice president always calls a new P-card user to "verify" the first purchase: "Just checking that it was you who bought that case of toner at Office Max…" — a not-so-subtle way of telling the cardholder "We are watching purchases made on your card!"

Education and Training

- Your organization is responsible for charges made until a card is reported as lost or stolen
- Educate employees about the importance of timely reporting on lost or stolen cards
- Educate your business cardholders to be on the lookout for unauthorized transactions, and be vigilant about monitoring card statements on a timely basis — fraudsters may "ping" an account with a small purchase to see if the transaction goes through before escalating the attack
- Some organizations have a tip line so whistle-blowers can report misuse of P-card

[7] Level III data is summary data and line item detail in addition to Level I and Level II data. Refer to individual card brands' websites for details on what is included in each Level.

Bank Services that May Help a Small Business Combat Payments Fraud

Talk to your banker to find out what fraud protection services and risk mitigation tools your bank offers and how they work. Some of these services may be available free of charge.

Examples of services commonly available from banks include:

- Account alerts
- Account masking services
- Dual authentication/multi-factor authentication for logging in to online banking and for initiation of payments
- Out-of-band authentication (refers to the use of two separate networks working simultaneously to authenticate a user, such as using a text message sent via a smart phone to verify the identity of the purchaser in a web transaction)
- Online information services (e.g., statements, check images)
- Fraud loss prevention services (e.g., insurance)
- Payments fraud prevention training
- ACH debit blocks
- ACH debit filters
- ACH positive pay
- ACH payee positive pay
- Check positive pay/reverse positive pay/positive pay with payee verification
- Post no check services
- Card alerts

Tips to Avoid Accepting Fraudulent Cards in Your Small Business

Today many customers prefer to pay with cards when they buy something. Small businesses that accept cards may become more competitive and may potentially increase sales. However, small businesses that accept card payments do expose themselves to potential losses from card fraud.

Tips that may help your small business lower the risk of accepting fraudulent cards:

- Learn to accurately identify payment cards by familiarizing yourself and your employees with legitimate cards. Visit the official websites of Visa®, MasterCard®, Discover® and American Express® to learn about features of their cards.
- Make sure there has been no tampering with the signature strip
- Look for a valid expiration date
- Don't accept an altered card
- Don't proceed with the sale if the customer's card is declined
- Don't agree to split a sale among multiple cards
- It is a best practice to always give the customer a receipt
- When processing a card-present payment, swipe the card through the POS terminal and verify that the account number on the terminal matches the account number on the card. Compare the name that prints on the receipt to the name embossed on the card, and compare the signature from the customer to the signature on the back of the card. If they don't match, don't continue with the sale.
- Get an authorization for the full amount of the sale
- If the card is unsigned, ask for a photo ID and check that the name on the ID matches the name on the card. Avoid accepting unsigned cards.

Tips to Avoid Accepting Fraudulent Cards in Your Small Business (continued)

- For card-not-present transactions (such as telephone orders, mail orders or internet/e-commerce sales), require the customer to provide the name on the card, billing address, card number, expiration date and the security code on the card.
- Know your customers and be aware of unusual activity such as a new customer requesting a high-dollar order, asking for rushed or overnight shipping, trying to rush or distract you or exhibiting odd behavior. Be suspicious of customers who appear to be working as a team. Watch out for customers who make a purchase and then leave the store, only to return later to buy more. Be suspicious if a customer buys a wide variety of merchandise, or very expensive merchandise and doesn't ask questions.
- Establish a card acceptance policy for your business and make sure your employees are familiar with it and follow it.
- Establish an escalation procedure with employees. Tell them who they should notify and educate them about resources they have at their disposal to verify cards.
- Protect your passwords and access codes by storing them in a safe location not easily accessible to others. Follow recommendations for strong passwords by using a lengthy combination of letters, numbers and special characters. Change passwords frequently.
- Keep track of documents associated with the transactions you process, including receipts, invoices, shipping confirmations, etc.
- When shipping a product, be sure the billing and shipping zip codes match; if they don't match, the customer should explain why. Don't accept the sale if you are suspicious.
- When shipping a product, be sure to keep tracking data and a delivery receipt. If the value of the shipment is high, require a signature upon delivery.
- Be cautious about accepting international orders.

Avoid internal card fraud:

Keep card data secure so employees cannot misuse the information. Be sure your system does not show the full card information (personal account number, cardholder name, expiration date, etc.) Processing a return is a common way of committing internal credit card fraud. A best practice is to not allow unmatched returns (returns that don't match a previous sale). Permit only trusted employees to handle returns.

Disputes and Chargebacks

A consumer has the right to dispute any charge on her credit card statement up to six months past any implied warranties. When a dispute occurs and the charge is reversed, this is called a chargeback. Be sure your business name is recognizable on the receipt: customers are more likely to file a dispute if they don't recognize the name on their card statement. Provide a telephone number for customers to call if they want more information about a charge. When processing payments and sending receipts, accurately describe the goods and/or services that you have provided. Provide adequate detail so the customer remembers the purchase and will be less inclined to file a dispute.

Tips for handling chargebacks:

- Set realistic customer expectations
- Put all of your refund/return policies in writing and provide to customers
- Promptly address customer issues and complaints
- Organize and securely store credit card receipts
- Respond promptly to retrieval requests

See "What Small Businesses Should Know about EMV or Chip Cards" on pages 30-31 to learn about fraud considerations related to the acceptance of EMV or chip cards.

Educate and Train Employees to Avoid Payments Fraud

Consider implementing these payments security best practices:

- Educate your employees about how to avoid payments fraud.
- Make sure your employees know never to divulge their user names or passwords. Phishing attackers may try via telephone calls or emails to deceive you into providing this by impersonating your bank. Your financial institution will not ask you to provide them with certain information (such as online banking user name, password or social security number) outside of the official online banking channel log-in.
- Use a dedicated PC for online banking. To avoid infecting this PC with viruses and malware, do not allow this PC to be used for social media (Facebook®, Instagram™, etc.), checking personal or business email, surfing the web or online shopping.
- Perform daily reconciliation of all bank accounts to help monitor for suspicious activity. This will allow you to return any fraudulent checks and ACH items in a timely manner.
- Keep anti-virus and malware detection software up-to-date; install security apps on mobile phones used by your employees.
- Use dual control for origination of ACH files and wire transfers. This means assigning roles to two different individuals so it is not possible for one person alone to complete a transaction.
- Shut down your work PC(s) at night.
- Follow recommendations for strong passwords by using a lengthy combination of letters, numbers and special characters. Change passwords frequently.
- Don't open email attachments or click on links in emails from someone you don't know.
- If you receive an email from someone you don't know, or if the tone of an email seems suspicious, use your mouse to hover over the name of the sender, and the full email address of the sender will display. Verify that the domain name of the user's email address looks valid.
- Be cautious about sharing personally identifiable information, especially on your website. Look at your website content with a suspicious eye: what information are you sharing with fraudsters?

Avoiding Data Breaches

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank account details, personal health information and other sensitive information. When it comes to data breaches, cyber criminals continually change their methods of attack; your defenses must adapt too.

Consider conducting an internal review to determine what customer data you are collecting and storing, and why. Consider whether you need to be collecting and storing this data. Realize that most states have data breach liability laws. You may be exposing your small business to unnecessary risk by collecting and storing certain customer data.

To help address concerns about data breaches, your small business might consider implementing (or working with a vendor who can implement on your behalf) the following mitigants:

- Defined policies and procedures regarding data security
- Security awareness training for employees
- Web content filtering and blacklisting
- Email attachment virus checking and filtering
- Restricted public access to company directories
- Application vulnerability scans
- Penetration testing
- Internet Protocol (IP) blacklisting
- Firewalls
- Data loss prevention tools
- Anti-virus, anti-spyware and anti-spam programs
- Limit personally identifiable information on your public website
- Multifactor authentication
- Restrictive administrative rights
- Monitoring
- Change default credentials
- Controlled use of administrative privileges

Hot Topics in Payments Fraud

Fighting card-not-present fraud

The U.S. is in the midst of migrating to the Europay, MasterCard and Visa (EMV) chip card standard, which is already proving to be effective in combating counterfeit card fraud. However, e-commerce merchants should be prepared as fraudsters shift their focus to card-not-present (CNP) fraud. In CNP transactions (which includes e-commerce and telephone orders), the merchant cannot inspect the plastic card (debit, credit or prepaid) when an order is submitted and payment initiated. Small businesses that are currently selling online, or are contemplating on doing so, will need to start implementing a strategy to combat CNP fraud.

How to help protect against CNP fraud

- Talk to your website administrator or service provider to make sure that any stored payment data is encrypted and that payment data is sent through a secure connection. (Subject to the card provider's agreement with the merchant and the Payment Card Industry Data Security Standard)
- Work with your web storefront service provider to implement secure payment options while balancing customer tolerance for "friction" at checkout.
- Ask your web storefront service provider and/or acquirer what CNP fraud risk mitigation tools they use and what risk measures they are applying to transactions.
- Implement multi-factor authentication and fraud prevention tools.[8]
    - Multi-factor authentication uses two or more methods to identify the cardholder:
        - Username and password
        - Knowledge-based questions
        - Address verification – (AVS) verifies the billing address of the cardholder
        - Card verification number (CVV) – three-digit value on the back of a card
        - Device authentication – registers a customer's known device to verify identity (i.e., laptop or mobile phone)
        - One-time passwords (OTP) – uses a password that is valid for only one session or transaction
        - Geolocation – identifies the geographic location of a person and/or device
        - Biometrics (i.e., thumbprint, facial or voice recognition)
    - Fraud Prevention Tools[9]
        - 3-D Secure – A proprietary industry standard messaging protocol used to verify identity in online credit and debit card transactions. Each card network has developed its own product based on the 3-D Secure protocol – Verified by Visa, MasterCard SecureCode®, AMEX SafeKey℠ and Discover ProtectBuy℠. E-commerce merchants can work with their merchant acquirer to provide this extra layer of security when validating the cardholder's identity. An updated protocol release in October 2016 uses high-risk data analytics for authentication and one-time passwords (OTP) sent via voice, text or email.
        - Data analytics – Uses a product or service to analyze a payment transaction to determine if it is likely to be fraudulent.
        - Behavior analytics – Helps detect fraud by monitoring consumer behavior on a website to detect suspicious and unusual activities. Can you identify your client if the payment is later returned?
        - Tokenization – Technology that replaces card data with substitute values (tokens) that are unusable by fraudsters. Can help protect data at rest/stored and data in transit.
    - CNP fraud resources:
        - "Forecasters Predict the New 3-D Secure Will Be More Popular Than Its Predecessor," by Jim Daly, Digital Transactions News, Oct. 31, 2016
        - https://www.emvco.com/faq.aspx?id=305
        - CardNotPresent.com

[8] Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud," Version 2, July 2016, EMV Migration Forum White Paper. See http://www.emv-connection.com/downloads/2015/04/CNP-Solutions-White-Paper-Version-2-FINAL-July-2016.pdf

[9] Ibid.

Ransomware

Ransomware, while not a new type of cybercrime, is on the rise and small businesses are not exempt from this fraud. The Federal Bureau of Investigation (FBI) defines ransomware as a "type of malware installed on a computer or server that encrypts the files, making them inaccessible until a specified ransom is paid. Ransomware is typically installed when a user clicks on a malicious link, opens a file in an email that installs the malware or through drive-by downloads (which does not require user-initiation) from a compromised website."[10]

To underscore the growing threat of ransomware, here are some findings from December 2016 studies[11,12]:

What to do if you are a victim of ransomware

- Disconnect the infected devices from your network to keep ransomware from spreading.[13]
- The FBI advises that you not pay the ransom. There is no guarantee that the fraudsters will provide the key to decrypt the data after they have been paid. There is no way to know if your data was copied or sold; it could be used for future attacks.
- Contact your local law enforcement.
- Report the incident on the FBI's Internet Crime Complaint Center (www.ic3.gov). By adding relevant information to their database, the FBI is learning more about the threat, who is behind the attacks and how criminals are identifying or targeting their victims.

How to help protect against a ransomware attack

- Back up your data regularly and verify the integrity of the backup.
- Secure your backups and ensure that they are not connected to the computers and networks they are backing up.
- Educate all staff on ransomware, and the danger of clicking on links and attachments contained in unsolicited emails.
- Regularly install upgrades and patches for operating systems, software and firmware.
- No users should be assigned administrative access to accounts unless absolutely needed.
- Configure access controls that give individuals appropriate read or write-access to files or directories only as needed.
- More recommendations can be found at: https://www.ic3.gov/media/2016/160915.aspx and https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

Ransomware resources:

- Federal Trade Commission: Ransomware – A Closer Look and How to Defend Against Ransomware
- FDIC: Cyber Challenge: A Community Bank Cyber Exercise
- McAfee: Understanding Ransomware and Strategies to Defeat It

[10] https://www.ic3.gov/media/2016/160915.aspx
[11] http://www.usatoday.com/story/tech/news/2016/12/14/2016-year-ransomware-bitcoin-ibm/95383786/
[12] http://www.cnbc.com/2016/12/13/ransomware-spiked-6000-in-2016-and-most-victims-paid-the-hackers-ibm-finds.html
[13] How to Defend Against Ransomware," by Ben Rossen, Federal Trade Commission, Nov. 10, 2016

Business email compromise

Business Email Compromise (BEC) scams typically target businesses that make routine wire transfers or that have foreign suppliers and businesses. Fraudsters start by compromising a legitimate business email account through social engineering or computer intrusion techniques. They gather company information by searching the internet, company websites and Facebook®, Twitter®, LinkedIn® and other social media sites. They then send "phishing" emails to get more detailed information about the business or individual.

Businesses need to be especially vigilant about "spear phishing" that directly targets business owners and key employees with access to financial information. Fraudsters create a fictitious email from a spoofed account with a forged sender address. They email a request for a payment that often mimics the style of the Chief Executive Officer (CEO) or Chief Financial Officer (CFO); the email is targeted to the person that handles wire transfers within the company. The email is often sent at the end of a business day or work week, or when executives or business owners are out of town. It states that it is urgent and confidential, and instructs the person to send a wire transfer. Because it appears to be legitimate, employees are deceived into making a payment to the fraudster's account. Wire transfers move very quickly and the funds are difficult to retrieve, making this type of fraud difficult to stop before funds are moved.

What to do if you are a victim of BEC

- Immediately contact your financial institution (FI) and request that staff there contact the corresponding FI where the transfer was sent.
- Contact the FBI. If the transfer is recent, the FBI will work with the Financial Crimes Enforcement Network (FinCEN) to try to return or freeze the funds.
- File a detailed complaint with the FBI's Internet Crime Complaint Center (www.IC3.gov) and identify the incident as a "BEC" scam.
- Find more information on contacting the FBI and filing a complaint with IC3 at: https://www.ic3.gov/media/2016/160614.aspx

How to help protect your business against BEC

- Establish strong policies and procedures for your payment processes and follow them (i.e., confirm requests for funds transfers, require out-of-band verification for significant transactions, etc.)
- Educate your staff on BEC.
- Be careful when sharing information on social media and on your company's website.
- Be vigilant and suspicious of emails that request secrecy and urgency.
- Avoid using free web-based email accounts and do not use the "reply" button when responding to business emails; instead use the "forward" button and send to an address from your contacts.
- The FBI has a more detailed list of best practices to protect against BEC scams at: https://www.ic3.gov/media/2016/160614.aspx

Source: Federal Bureau of Investigation Public Service Announcement

The U.S. is one of the last developed countries to migrate from magnetic-stripe ("mag-stripe") cards to EMV[14] or chip cards The four major card brands (American Express, Discover, MasterCard and Visa) led the effort to move the U.S. to a chip-based card payments infrastructure. Affected are credit, debit and prepaid cards issued by U.S. financial institutions.

Benefits of Chip Cards and Impact on Card Fraud

The biggest benefit of chip card technology is the potential reduction in card fraud due to counterfeit, and lost and stolen cards for card-present transactions (card-present transactions refer to sales in which the card is physically present at the POS and the merchant has the opportunity to inspect the card.) Chip card transactions offer enhanced functionality in cardholder verification and transaction authorization, thus potentially providing better security than mag-stripe cards.

A chip card has an embedded microprocessor chip (it looks like a small, metallic square on the front of the card) that stores information securely and performs cryptographic processing during the payment transaction.

When a chip card is manufactured, the chip is encoded with security credentials that are extremely difficult to counterfeit. Notably, the chip creates dynamic data that are unique for each transaction and these data cannot be used again, thus diminishing the value of stolen card data. Because of these security features, countries that have implemented chip cards have seen a reduction in card-present fraud rates.

Traditional mag-stripe cards, in comparison, carry static data that does not change from one transaction to the next. Criminals steal the data from the mag-stripe and use it to create fraudulent transactions. For example, criminals may install devices to skim card data at automated fuel pumps or Automated Teller Machines (ATMs) and then use that card data to make fraudulent purchases.

In card-not-present (CNP) transactions (such as telephone, mail orders and internet sales), the merchant doesn't see the actual card. EMV technology does nothing to protect against fraud in CNP transactions. Countries that have migrated to chip cards have seen CNP fraud rates increase. Criminals who are thwarted by the more secure card-present transaction environment that comes with chip cards may turn their attention to the CNP environment where the pickings are easier. Similarly, cross-border counterfeit fraud (particularly ATM fraud) rates have grown in countries that have moved to chip cards. Card issuers, merchants, card brands, cardholders and others should consider implementing a variety of potential solutions[15] to help mitigate or prevent CNP fraud.

[14] EMV, which stands for Europay, MasterCard and Visa, is a global standard for integrated circuit or chip cards. The EMV specifications define a set of requirements to ensure interoperability between chip-based cards and terminals throughout the world.

[15] EMV Migration Forum, "Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud," March 2016, available at www.emv-connection.com/near-term-solutions-to-address-the-growing-threat-of-card-not-present-fraud/. This white paper is an educational resource on best practices for authentication methods and fraud tools to secure the CNP channel as the U.S. migrates to chip technology.

Fraud Liability Shift

A major incentive for merchants to prepare for chip card acceptance is the shift in liability that took effect in October 2015. Previously, under the card brands' operating rules, the card issuer was liable for financial losses due to counterfeit card fraud. With the liability shift, a merchant will bear the loss if the issuer has issued chip cards to its cardholders and if that merchant has not been certified through its acquirer as being EMV-compliant (by having implemented payment terminals that can read chip cards and taking other compliance steps).[16]

Also in October 2015, MasterCard, Discover and American Express shifted the liability for a lost or stolen card to the party with the highest risk environment. Within that hierarchy, chip and PIN verification is considered more secure than chip and signature. If neither or both parties are EMV compliant, the fraud liability remains the same as it is today.

Accepting Chip Cards at the POS

Many POS terminals purchased in recent years are already EMV-capable, but that functionality is not turned on; it is necessary for merchants to get the necessary software installed, tested and certified before they can process chip card transactions. Depending on the market, there may be a long wait for installation, testing and certification services.

As a small business, is it advisable for you to invest in POS terminals or upgrades so your business can accept chip cards? Investment in chip-card acceptance equipment may be worthwhile if:

- You accept card payments today in "card-present" situations, or you plan to do so in the near future
- A significant portion of your sales is to strangers (versus people you know and trust), making your business more vulnerable to counterfeit and lost/stolen card fraud attacks
- Card payments are a significant percentage of your total sales
  - However, if most of your card transactions tend to be telephone orders or internet purchases (CNP transactions), it may not be cost-effective for you to invest in chip card terminals

Another consideration is the time and resources needed to train your staff and educate customers on the use of chip cards. In addition, some consumers may perceive that chip cards offer better security. Merchants that don't accept chip cards could be at a disadvantage if they are viewed as a less secure option for that consumer, potentially eroding customer confidence and reducing loyalty.

It is important to realize that nearly all chip cards (whether issued in the U.S. or elsewhere) will continue to carry mag-stripes for the foreseeable future, and the U.S. payments infrastructure will continue to support mag-stripe technology for many years to come. Thus, merchants will still be able to accept card payments (and process them with mag-stripe technology) even if their POS terminals are not equipped to accept chip card transactions

To Learn More about Chip Cards

Small businesses can prepare for the move to chip cards by learning more about issues, costs and arming themselves with facts to support informed business decisions. The websites http://www.emv-connection.com/us-payments-forum/ and www.gochipcard.com offer useful information. Seek out information from card brand representatives and card brand websites, and confer with bankers, merchant acquirers and card processing service providers to inform your decision on whether and when to accept chip cards. See the Resources section on page 40 for additional links to information about chip cards.

[16] The principle is that the party (issuer or merchant) that is the cause of a contact chip transaction not occurring (and thus falling back to a magnetic stripe transaction) will be financially liable for any resulting card-present counterfeit card losses.

ONLINE AND MOBILE PAYMENT ALTERNATIVES

Many small businesses utilize online and mobile financial services offered by their banks or other service providers for incoming and outgoing payments. If a small business wants its customers to have the option of paying via online bill pay, it works with its bank to be added to the relevant biller directory for payees, along with pertinent payment instructions. As a payer (when the business initiates a payment from its bank account), a business can control when the payment is withdrawn from its account. Online bill pay is usually free to use.

There are obvious benefits to being able to access services such as online bill payment and transaction history. However, there are some potential concerns. For example, when using online bill pay, businesses should keep in mind that they are not protected by Regulation E (Reg E)[17] in the same way as consumers. If an online business account is hacked and a fraudulent payment is issued, the business may be liable for the loss. Dual controls[18] are not usually offered, so online bill pay might be vulnerable to employee fraud. In general, when considering online payments, businesses should be aware of some of the many different schemes that are used in cyber-attacks against business information and accounts. Convenience and increased access brought about by online and mobile payment options go hand in hand with considerations for how to ensure that payments are secure.

It is especially important to impose access controls in order to limit the parties that can see and store data transferred via card transactions accepted on mobile devices. For more on payments fraud prevention, refer to pages 21 to 29 of this Toolkit.

There are a variety of online payment options for small businesses to consider. For example, Amazon Payments® integrates into a business' existing website; customers can pay using information stored in their Amazon.com accounts. Another option is authorize.net, which is a payment gateway service provider that works with a business' existing merchant account to accept credit cards and electronic checks through its website. Many small businesses are familiar with Intuit's Billing Solution which integrates directly with QuickBooks and allows a business to get paid online via credit card from any invoice generated.

In addition, there are various payment services that small businesses can access using mobile devices such as smart phones and tablets. Features include access to account information, alerts, collection of card payments via attachable appliance or app, the ability to make payments and remote deposit capture of checks.

There are a variety of online and mobile payment options, with obvious benefits and some potential concerns, for small businesses to consider.

[17] Regulation E or Reg E provides a basic framework that establishes the rights, liabilities and responsibilities of participants in electronic fund transfer systems such as automated teller machine transfers, telephone bill-payment services, POS terminal transfers in stores and preauthorized transfers from or to a consumer's account (such as direct deposit and social security payments). The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer or magnetic tape that instructs a financial institution either to credit or to debit a consumer's asset account. Source: www.federalreserve.gov/bankinforeg/regecg.htm

[18] Dual controls means requiring more than one person to act to make payments on behalf of a business.

ONLINE AND MOBILE PAYMENT ALTERNATIVES

Following are examples of pay-as-you-go payment aggregators that have similar offerings: PayPal,® Stripe® and Square®. These alternatives are marketed to small merchants as ways to accept low-value credit and/or debit card payments at fixed rates without requiring a merchant account. More information to help small businesses research merchant accounts and online and mobile card processing solutions is available in the Resources section on page 41.

Detailed Example of an Online Credit Card Processor: PayPal®

In 2015, there were 188 million active PayPal accounts in 202 countries.[19] PayPal allows small businesses to accept online payments without having a traditional merchant account. Customers don't need a PayPal account to pay. PayPal charges its business account holders a per-transaction fee, plus a percentage of the transaction. Through PayPal business services, businesses can accept credit cards online, at the register or by phone; they can also create and track secure invoices through a PayPal account. The system has recurring payment capabilities.

PayPal features include:

- Businesses can create and send invoices through PayPal account
- Capability of setting up recurring payments
- Ease of setup and use
- Customer familiarity
- No merchant account needed
- Flexible card processing for businesses with low-volume sales
- Customers don't need a PayPal account to make a payment
- Can be integrated with other shopping cart systems
- Transparent with terms and pricing
- 24/7 phone and email support

Concerns include:

- PayPal's Seller Protection policies do not cover digital goods[20]
- Cost of chargebacks
- Time for funds to clear
- Limits of terms of use policy
- Quick to hold sellers' funds if fraud is suspected
- PayPal is not regulated in the same way that banks are regulated; protections differ
- Fees for currency exchange

PayPal also has a mobile/cloud tokenization[21] solution: the consumer opens a mobile app, authenticates with the payments services provider (PSP) and requests an offline payment token.

[19] Source: "How PayPal Is Taking a Chance on AI to Fight Fraud," by Penny Crosman, AmericanBanker.com, September 1, 2016

[20] Digital goods are intangible goods that exist in digital form, such as e-books or webinars.

[21] Tokenization is the process of substituting sensitive data with unique identification symbols (a "token") that retain all the essential information without compromising security. The token has no extrinsic or exploitable meaning or value.

Detailed Example of an Online Credit Card Processor: Stripe®

Stripe offers a credit card processing solution that does not require a merchant account. It allows a small business's online store to start processing credit card sales right away. A business can choose from a simple checkout system that they can copy and paste in to their online store, or program the Stripe Application Programming Interface (API) into their shopping cart. Various features and customization options allow a business to tailvor the Stripe service to suit its unique e-commerce needs. Pricing is straight-forward and only kicks in when a sale is made. The chargeback fee is relatively low and a dispute system is in place to protect sellers from fraudulent claims. To start using Stripe, a business signs up for an account, provides business and bank information, activates the account and chooses a processing method. Funds go directly into the business' bank account. Customers of the online store enjoy a hassle-free checkout experience. Card details can be saved so customers can pay again with a single click. In addition to enabling online card purchases, Stripe also works for phone and mail orders.

Concerns include:

- Payments have taken seven days to process, although a two-day turnaround is advertised
- Access to the customer support team is via email first, then a rep will solve the issue online or call

Detailed Example of a Mobile Credit Card Processor: Square®

Square uses mobile apps through phones for Android™ and/or Apple® to allow buyers to pay via card (Square accepts Visa, MasterCard, American Express and Discover) at places like farmers markets, restaurants, festivals and other venues with small merchants. Square utilizes equipment (the "dongle") and apps that are fairly easy for small businesses to "plug in" and use; examples of how Square works are included below. Moreover, Square does not require a merchant account, unlike most credit card companies. Square accounts are linked to merchants' bank accounts, and deposits into those accounts are usually available in one or two business days. Square charges businesses a flat rate per swipe plus a percentage of each transaction; rates are higher for manually-keyed transactions.

Square offers merchants a variety of ways to access card payments:

- Square Reader: This is a small "dongle" that attaches to an iPhone® or smartphone for Android's headset jack; the Square app is used to access payment capabilities. Customers can swipe the card and enter their PIN or provide a signature right on the phone screen. A Square Reader can be obtained for free.
- Square NFC/EMV Reader: Square has partnered with Apple to allow merchants to accept Apple Pay® (and other contactless mobile payments) and EMV chip payments. It can be used in place of or with the Square Reader and uses the same app to process payments.
- Square Register: The Square Register app allows merchants to use the Square Reader on an iPad® or tablet for Android to move beyond processing card payments. Square Register allows a variety of services such as: accepting cash payments; sending digital receipts and invoices; and processing transactions offline, among other services.
- Square Stand: This alternative allows a merchant to turn an iPad into a stationary POS system at the checkout. The Square Stand has a built-in reader that can be turned to face the merchant or the customer.

A BRIEF INTRODUCTION TO VIRTUAL CURRENCIES

Virtual currency (also referred to as digital currency) can be defined as a type of stored-value product or digital money that is issued and usually controlled by its developers, and is used and accepted among the members of a virtual community. Virtual currencies are not issued by a federal government ("fiat currency") or backed by a central bank. Consequently, virtual currency is generally unregulated. There are currently more than two hundred virtual currencies in use, of which Bitcoin is the largest and most well-known. Small businesses that are thinking about moving to electronic payments should consider whether or not accepting virtual currencies as a form of payment makes sense for them.

Virtual currencies, which are non-fiat digital moneys normally controlled by their developers, fall into three categories: closed schemes, unidirectional and bidirectional:

- Closed currencies are not exchangeable with traditional currencies (an example is World of Warcraft® gold).
- Unidirectional currencies are bought with traditional money or can be earned by participating in activities (Amazon Coins are an example) but cannot be converted back to fiat currency.
- Bidirectional currencies are purchased with traditional money and can be converted back to traditional money; they can be used to buy virtual and non-virtual goods. Bitcoin is an example of bidirectional virtual currency. This is the only type of virtual currency that might have the potential to compete with traditional currency. Bitcoins act as currency in that they can be used as a means of payment, a method of exchange, a store of value and a unit of account.

Virtual Currency Example: Bitcoin

Bitcoin, a virtual currency system with no central authority at its core, was launched in 2009. It permits the transfer of currency online, directly, anonymously and outside government control. Bitcoin has attracted much attention from computer developers, venture capitalists and merchants who see it as an alternative to traditional payments. Transactions take place using complex mathematical algorithms and elliptic-curve cryptography, including digital signatures, open source computing methods and peer to peer networks. Transactions are recorded in the "blockchain," a public ledger and proof of every Bitcoin transaction that has ever occurred. New Bitcoins are created through "mining," as a reward for applying computing power to verify new transactions. The average person can't really be a Bitcoin miner, because of the computing power now required. Instead, people buy and sell Bitcoin on a number of exchanges, privately through peer-to-peer contact. Some people who are interested in Bitcoin don't exchange it for currency at all, but offer goods and services for Bitcoin.

Bitcoin can be divided to eight decimal places (to a "satoshi" currently worth less than 1/1,000 of a cent) so that it can accommodate so-called microtransactions for low-value transfers. Today, about 15.3 million Bitcoins are in existence. A finite supply of 21 million Bitcoins will be created through mining, at which point the total amount of Bitcoin in circulation will no longer increase; it will likely decrease slightly as some people will inevitably lose their private keys, essentially destroying the Bitcoin they owned by locking it away forever. Because of this feature, some people call Bitcoin "deflationary by design," meaning that it is intended to appreciate in value over time, assuming increased adoption makes it relatively more scarce. When miners are no longer rewarded for operating the network by newly created coins, they will rely entirely on transaction fees (which are a relatively small portion of revenue today, and just a fraction of the cost of traditional payment networks).

Some merchants accept Bitcoin as payment today. Examples include:

- Overstock.com – since Bitcoin payments save the retailer credit-card fees, Overstock™ offered an incentive to customers paying with Bitcoin; 1% back on purchases (in-store credit)
- Microsoft® accepts Bitcoin payments for a variety of digital content
- Dell® allows customers to buy computers and hardware with Bitcoin
- DISH Network® has announced it will allow customers to pay for their television programming packages with Bitcoin
- Expedia® accepts Bitcoin for hotel bookings (but not for flights, yet)
- Square's online marketplace, Square Market
- Many others accept Bitcoin payment directly; other retailers offer their dollar-denominated gift cards through online sellers (like Gyft) who accept Bitcoin.

A key barrier to the acceptance of any virtual currency is the desirability of actually holding revenue denominated in that currency. Most merchants contract with an exchange (e.g., Coinbase®), that converts consumers' Bitcoins into dollars and transfers dollars to the merchant. Bitcoin does not allow chargebacks and Bitcoin transaction costs are generally cheaper than those with credit/ debit cards: the fee for a service like Coinbase is around 1%. However, the transaction fee to Square Market merchants for payments with Bitcoin remains the same as the fee charged for all other Square Market transactions.

Bitcoin is more than a currency: it also acts as a payment system. Transactions are tracked and audited for legitimacy through open-source code; they are final and irrevocable. There are also escrow services to mediate transaction disputes between buyers and sellers. Because it is decentralized, some tout its advantage in cross-border transfers, which are processed as easily as domestic payments. One can envision Bitcoin as an extension of other innovations that have changed the payment system, such as Amazon, PayPal and Square.

Issues to Consider

Some observers have identified potential benefits and risks associated with virtual currencies such as Bitcoin.

Potential Benefits of Virtual Currencies

- May reduce risk of identity theft
- Has immunity to conventional inflationary pressures and sovereign risk
- Gives potential access to financial instruments for those who are unbanked
- Might have lower transaction costs for merchants
- Settles almost immediately
- Provides irrevocability and finality
- Is accessible to anyone with access to a computer or smart phone
- Contains security features that are created through digital signatures and cryptography
- Useful in countries where social or political climate may lead to distrust of local currencies or there is a high degree of connectivity to the internet
- Opportunities in areas like notary services and tracking asset ownership

Potential Risks of Virtual Currencies

- May allow for a level of anonymity that can lead to criminal activity
- Can require a lot of computing power and electrical energy to complete a transaction because the calculations that assure trust between unfamiliar parties are rigorous
- Has no central authority providing a natural bridge to the currency and no guarantee of value
- Many provides no recourse for owners who lose money through fraud, exchange collapse, or simple transaction errors and lost “passwords”
- Is treated differently than other currency by regulatory bodies. For example, in the U.S., the Internal Revenue Service (IRS) has said that Bitcoin and other virtual currencies will be taxed like property, not currency.
- Faces an uncertain legal status. Regulations are still forming and inconsistent and some nations are attempting to outright ban the use of virtual currency.
- Is not ubiquitous

Despite issues and challenges, virtual currencies aren’t going anywhere. Virtual currencies are difficult to repress due to their decentralized structure. Some observers think virtual currencies could ultimately change not only the traditional financial system, but also the way we transfer and record financial assets like stocks, contracts, property titles, patents and marriage licenses. The same design features that allow virtual currencies to exchange value without relying on a central record-keeper make it possible for virtual currencies to be used for anything for which we have traditionally used a trusted “middleman” for verification. For example, in 2015, at a hotel at Walt Disney World®, a couple used a Bitcoin ATM to record their written marriage vows on the blockchain. Major stock exchanges and even government property records offices are already experimenting with these networks for recording and transferring ownership of stock certificates and property titles. Others are finding ways to use the networks to create “smart contracts” that can function as automated escrow services and more. Increasingly, industry experts believe that decentralized currencies might not become major factors themselves, but that the technology underlying their creation will transform traditional money and financial services and find application across a range of industries that manage identity, ownership, privacy and contracts.

Business Continuity Planning

On May 22, 2011, one of the top 10 deadliest tornadoes in the U.S. to date tore through Joplin, Missouri. This was the third tornado to strike Joplin since 1971 and the event included multiple vortexes and 200 miles per hour (MPH) winds. Over 17,000 insurance claims were filed with over $2.2 billion paid. Would your business survive such an event? How would you and your employees work around the loss of major city infrastructure, power, phone, water outages and internet? How would you react to hazardous conditions including natural gas leaks and harmful spills?

"Locating the business was a challenge: no landmarks, street signs, or visual reminders remained. There were no phones and no internet. Cell service was spotty; at least texting was often successful. It was difficult to find our office when there were no street signs."

– From October 2012 EPCOR presentation "Business Continuity Planning: Lessons from the Joplin Tornado" by representatives of Commerce and Arvest Banks.

According to the Institute for Business and Home Safety, an estimated 25 percent of businesses do not reopen following a major disaster. You can protect your business by identifying the risks associated with natural and man-made disasters, and by creating a plan for action should a disaster strike. By keeping those plans updated, you can help ensure the survival of your business.

Business continuity is your plan to keep working despite almost any disruption or disaster. It involves the ability to keep or get your processes and information back up and running as soon as possible. This can be accomplished by something as simple as restoring a backup to a new computer (so your whole system is back the way it was), all the way up to using a virtual service with your backup in the cloud. Business continuity is a must for companies of all sizes. The ability to quickly get your system working on current or new devices can ensure your business will survive not only the event, but the potential long-term effects.

Disaster recovery is the ability to get back to normal operations in the event of a disaster. A disaster can be anything from a storm or flood that destroys your office to a breach of your sensitive networks or a compromise at your point-of-sale. Disaster recovery is really just a plan to put the information critical to your business onto new computers and/or servers.

Backing up your data must be a priority for your disaster recovery planning; your backups are what you're going to use to recover after the disaster occurs. Backups can include a variety of methods: files, directories, image backup, cloud storage, etc. It is common to experience a hardware or software failure causing you to lose your data. Backing up information from your personal computer (PC) regularly is recommended so you do not lose important information. This practice can also protect you from fraud issues such as malware used to hold your data hostage for a ransom. This may also include backing up the data on your mobile devices, such as photos and contacts.

"Locating the business was a challenge: no landmarks, street signs, or visual reminders remained. There were no phones and no internet. Cell service was spotty; at least texting was often successful. It was difficult to find our office when there were no street signs."

Remember: What you backed up determines what you can recover.

Planning ahead for a business-threatening event should include an "all hazards" approach. There are many different threats or hazards. The probability that a specific hazard will impact your business is hard to determine. That's why it's important to consider many different threats and hazards and the likelihood each will occur. Strategies for prevention/deterrence and risk mitigation should be developed as part of this planning process. Threats or hazards that are classified as "probable" and those hazards that could cause injury, property damage, business disruption or environmental impact should be addressed.

Write out our plan and testing strategies. Once you've identified the key factors in your recovery and continuity planning, it's time to start setting up your plan. Begin by establishing requirements and objectives for your disaster recovery plan and capturing them in a written policy document. A preparedness policy that is consistent with the mission and vision of the business should be written and disseminated by management. The policy should define the goals and objectives of the program, and roles and responsibilities. The policy should authorize selected employees to develop the program and keep it current. Each of your major stakeholders needs to review the document and edit it as needed. You'll also want to establish testing processes and periodically review your strategy. In general, it's a good idea to test your backup strategy once a quarter just to make sure that everything is running smoothly and to verify that no significant changes are needed. Persons with a defined role in the preparedness program should be trained to do their assigned tasks and all employees should be cross-trained so they can take appropriate protective actions during an emergency.

WHAT SHOULD A BUSINESS CONTINUITY PLAN OUTLINE?

- **Who is responsible for testing?**
- **When tests will take place?**
- **What will be restored in a test?**
- **How backup will be restored?**

Before disaster strikes, have conversations with your banker, accountant and other financial services providers to find out what their disaster recovery plans are. Online banking services such as bill pay, remote deposit services or even credit card access can help your business function from any internet or mobile connection. Determine how they will support your ability to recover from disasters in order to assure the continuity of your small business.

Disaster Recovery is a lot like insurance – you hope you never need it but you want to make sure you have it if you do. While natural disasters, such as hurricanes and floods, tend to grab more attention, most forms of data loss and downtime have nothing to do with weather. Don't overlook threats such as fraud, water damage or fire.

Learn more about preparing a disaster recovery plan for your small business by exploring the business continuity resources listed on page 41.

A SELF-ASSESSMENT QUIZ

Test how ready your small business is to better utilize electronic payments

Directions: Answer each yes/no question below. Toolkit sections are referenced if you want more information about a topic. When you are done, tally your score and find out how ready your small business is to reap the benefits of electronic payments.

1. Do you currently pay your employees via direct deposit for payroll or other expenses?

❍ Yes ❍ No

Reference: page 5 "Payment Types Explained: Automated Clearing House (ACH)"

2. Do you want to gain efficiencies by paying your bills with electronic ACH or card payments instead of writing checks?

❍ Yes ❍ No

Reference: page 6 "What Small Businesses Should Know about ACH"

3. Use of "dual control" or "separation of duties" is critical to protect your business from financial loss. Do you have two individuals (each with their own computer) at your business you can rely on, so one person can originate (create) the payment and the second person can authorize and release it? [Note: it is also wise to use dual control for any new account set-ups.]

❍ Yes ❍ No

Reference: page 22 "Fraud Prevention and Mitigation Tips: ACH Fraud"

4. Do you have a contact at your bank you can turn to for assistance to get started on using ACH origination or obtaining a purchasing card to make payments to suppliers/vendors?

❍ Yes ❍ No

Reference: page 12 "How to Talk to Your Bankers about Payments" and page 13 "Bankers, Small Businesses and ACH: Getting on the Same Wavelength"

5. Think about your current list of suppliers or vendors. Can you identify which you would like to or could pay electronically instead of by check?

❍ Yes ❍ No

Reference: page 10 "ACH Payments and Remittance Solutions"

6. Have you considered the need for trading partner agreements that you will want your suppliers/vendors to sign in order to authorize ACH or card payments?

❍ Yes ❍ No

Reference: page 19 "Can I Pay You by ACH? Sample Trading Partner Agreement to Start Receiving ACH Payments"

7. Have you identified the decision makers at your business who need to be influenced and persuaded in order to implement the change from checks to electronic payments?

❍ Yes ❍ No

8. Have you evaluated the hardware and software requirements (including those required by your bank) needed to access the ACH system?

❍ Yes ❍ No

Reference for 7 and 8: pages 14-17 "Tips on Getting Started Originating ACH"

9. Have you thought about the training your employees will need to learn how to originate ACH payments or start paying bills on a card?

❍ Yes ❍ No

Reference: page 23 "Purchasing Card Fraud Prevention" and page 26 "Educate and Train Employees to Avoid Payments Fraud"

10. If planning to pay your suppliers/vendors by card or ACH, have you thought about controls, review processes and employee training needed to validate the payee and ensure that all outgoing payments are legitimate?

❍ Yes ❍ No

Reference: pages 22-26 "Fraud Prevention and Mitigation Tips"

Scoring: For every "yes" answer give yourself 10 points.

100 points: Super! You are ready to proceed.

80 to 90 points: Excellent! You are nearly there.

60 to 70 points: Very good! Just a little more preparation is needed. Go back and study the Toolkit references listed above to learn more.

50 points or less: Good, but more preparation is needed on your part before proceeding.

Glossaries of Payment Terms

First Data Payments Industry Glossary: www.firstdata.com/downloads/thought-leadership/Payments-Glossary.pdf

TR-43-2014 Remittance Glossary:
A Publication of the Business Payments Coalition
www.x9.org/wp-content/uploads/2014/02/TR-43-2014-Remittance-Glossary.pdf
Vocabulary and terminology reference guide that defines 169 terms related to payables and receivables processing, business to business payments and remittance handling.

Cardinal Commerce Payments Glossary: http://info.cardinalcommerce.com/payments_a_to_z

Accounting payment terms: www.accountingtools.com/accounting-payment-terms

Credit and Debit Card Resources

PCI stands for Payment Cards Industry.

PCI compliance information for merchants: www.pcisecuritystandards.org/pci_security/why_security_matters

PCI DSS Quick Reference Guide:
Understanding the Payment Card Industry
www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

PCI Information Supplement:
Best Practices for Implementing a Security Awareness Program
www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf

Purchasing card basics: www.napcp.org/?page=PCardIntro

Recommended Communications Best Practices is a step-by-step resource for issuers and merchants to develop effective messaging and education approaches during the U.S. migration to chip technology.
Available on the EMV Connection website at www.emv-connection.com/recommended-communications-best-practices/

Advice on best practices for card acceptance:
www.squareup.com/help/us/en/article/5079-best-practices-for-accepting-payment-cards
www.transfirst.com/resources/whitepapers/tips-for-preventing-fraud-and-avoiding-chargebacks

EMV Cards or Chip Cards Resources

General information about chip cards:
www.gochipcard.com
www.emv-connection.com

Technical specifications for EMV: www.emvco.com

Information for merchants about chip card acceptance from the major card brands:

American Express: www209.americanexpress.com/merchant/services/en_US/payment-EMV

Discover: www.discovernetwork.com/chip-card/merchants/index.html

MasterCard: www.mastercard.us/en-us/merchants/safety-security/emv-chip.html

Visa: https://usa.visa.com/dam/VCOM/download/merchants/Visa-Merchant_EMV_Chip_Acceptance-2014-07-17.pdf

Examples of Information for small merchants from payments processors:
www.chasepaymentech.com/faq_emv_chip_card_technology.html
http://info.vantiv.com/rs/vantiv/images/emv_what_smbs_should_know_about_emv_whitepaper.pdf

Merchant Accounts

Examples of websites with reviews, ratings and comparisons:
https://www.merchantmaverick.com/
http://www.best10merchantservices.com/
http://www.toptenreviews.com/business/payment-processing/best-merchant-services/
http://www.businessnewsdaily.com/8061-best-credit-card-processing.html

ACH Resources

National Automated Clearing House Association website (NACHA): www.nacha.org/

Direct payment via ACH: www.electronicpayments.nacha.org/small-businesses

How to accept ACH payments: www.wikihow.com/Accept-ACH-Payments

Same Day ACH:

Learn more about Same Day ACH: www.frbservices.org/resourcecenter/sameday_ach/index.html
www.resourcecenter.nacha.org/

Watch the video "Same Day ACH: How Will You Benefit?": www.youtube.com/watch?v=K_XsiQ_54B0

Companies that Provide Payroll Services:
To find and compare payroll service providers, conduct an internet search using terms such as: payroll vendor comparison, payroll vendors reviews, payroll company comparisons, payroll service cost comparison, online payroll services reviews, outsource payroll service providers, compare payroll service companies, list of payroll providers, best online payroll service for small business, etc.

ACH Checklists and Forms

Direct Deposit of Payroll via ACH

Start-up information and ample form for employees to sign to start having pay checks directly deposited into checking and/or savings accounts:
www.electronicpayments.nacha.org/direct-deposit/businesses/direct-deposit-businesses#dd-biz-get-started

Information for employees on direct deposit:
www.electronicpayments.nacha.org/direct-deposit/consumers/direct-deposit-consumers

Direct payment via ACH

"Get Started Toolkit" is a checklist of steps to follow to get paid and make payments electronically via ACH:
www.electronicpayments.nacha.org/direct-payment/small-businesses/direct-payment-small-businesses

General Small Business Resources

America's Small Business Development Center: http://www.americassbdc.org/

Offers no-cost business consulting to small businesses.

America's Small Business Development Centers' website features an e-learning center with over 1,400 online business courses and video tutorials. A free membership offer is available.

Small Business Administration: www.sba.gov/
Follow this path to useful resources about payments: www.sba.gov/ » Starting & Managing » Managing a Business » Running a Business » Managing Business Finances & Accounting.

Business Continuity Planning:
www.sba.gov/managing-business/running-business/emergency-preparedness/emergency-preparedness
www.preparemybusiness.org/
www.ready.gov/business/implementation/IT

Fraud and Data Security Resources

Dun and Bradstreet "How to Help Prevent Payroll Fraud":
www.nfib.com/article/7-steps-to-preventing-payroll-fraud-57312/

Federal Communications Commission's Ten Cybersecurity Tips for Small Business:
https://apps.fcc.gov/edocs_public/attachmatch/DOC-306595A1.pdf

Create a free customized Cyber Security Planning guide for your small business:
www.fcc.gov/cyberplanner to create a free customized Cyber Security Planning guide for your small business and visit www.dhs.gov/stopthinkconnect to download resources on cybersecurity awareness for your business.

Chamber of Commerce's Internet Security Essentials for Businesses:
www.uschamber.com/sites/default/files/legacy/issues/defense/files/020956_PDF_web.pdf

Council of Better Business Bureaus' Data Security Made Simpler:
www.bbb.org/data-security/

Business Know-How's "Are Employees Stealing from You? Tips to Prevent Employee Theft":
www.businessknowhow.com/manage/employee-theft.htm

Association of Certified Fraud Examiners "Small Business Fraud Prevention Manual" ($59.00):
www.acfe.com/products.aspx?id=2155&terms=(small+business+fraud+prevention)+
This is a book providing information on the most common internal and external fraud schemes committed by customers, employees and vendors against small businesses, as well as tips on how to prevent these schemes from happening to you. Highlights include: cash receipts and disbursements fraud; inventory and merchandise thefts; employee fraud prevention techniques; check and credit card fraud; vendor fraud; and fraud perpetrator prosecution. Explains what to do if your small business becomes a victim to fraud, including avoiding liability when conducting investigations and taking civil actions against perpetrators.

"Payments Fraud Liability Matrix" and "2014 Payments Fraud Survey Summary of Consolidated Results" are available at:
www.minneapolisfed.org/about/what-we-do/payments-information

The Association of Certified Fraud Examiners (ACFE) offer free fraud resources: www.acfe.com/free-resources.aspx

ACFE "Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study":
www.acfe.com/rttn-occupational.aspx
Includes a section on methods used to detect fraud in small businesses, as well as summarizing the frequency of fraud schemes by industry.

The International Association of Financial Crimes Investigators (IAFCI) offers general education in "Fraud Smarts: A Practical Guide for Online Safety":
www.iafci.org/Public/Public_Awareness/Community_Cautions.aspx In addition, select the small business icon on the left of this page to see fraud prevention tips for small businesses, including how to create a cyber security plan.

Common Fraud Schemes
The Federal Bureau of Investigation (FBI) lists the most common scams that the FBI investigates and offers tips to help prevent being victimized by fraud at the following link. You can sign up for email updates from the FBI on breaking news and other topics. www.fbi.gov/scams-and-safety/common-fraud-schemes

Bank Holidays

Standard Federal Reserve Bank Holidays

Holiday*	2017	2018	2019
New Years' Day	Jan 2	Jan 1	Jan 1
Martin Luther King, Jr. Day	Jan 16	Jan 15	Jan 21
President's Day	Feb 20	Feb 19	Feb 18
Memorial Day	May 29	May 28	May 27
Independence Day	Jul 4	Jul 4	Jul 4
Labor Day	Sep 4	Sep 3	Sep 2
Columbus Day	Oct 9	Oct 8	Oct 14
Veteran's Day	Nov 11*	Nov 12	Nov 11
Thanksgiving Day	Nov 23	Nov 22	Nov 28
Christmas Day	Dec 25	Dec 25	Dec 25

* For holidays falling on Saturday, Federal Reserve Banks and Branches will be open the preceding Friday. For holidays falling on Sunday, all Federal Reserve Banks and Branches will be closed the following Monday.

Bank Holidays Sources:
Federal Reserve Bank holidays: www.frbservices.org/holidayschedules/
International bank holidays: www.bank-holidays.com

Regional Payments Associations

Regional Payment Associations (RPAs) serve member banks, credit unions, thrifts, municipalities, payment technology providers and businesses. Their services vary, but for the most part they all provide information, education, publications, operational support, advocacy and resources on Automated Clearing House payments as well as on other payment systems such as check and image; credit, debit and prepaid cards; wires; and payments-related risk and fraud.

Regional Payments Association	Website	General Territory Served
EastPay	www.eastpay.org	Florida, North Carolina, Virginia and West Virginia
EPCOR – Electronic Payments Core of Knowledge	www.epcor.org	Arkansas, Indiana, Kansas, Kentucky, Missouri, Nebraska, Oklahoma, Ohio, Illinois, Iowa, Pennsylvania and West Virginia
MACHA – the Mid-Atlantic Payments Association	www.macha.org	Maryland, the District of Columbia, Delaware, Northern Virginia, Northeast West Virginia and Southern Pennsylvania
NEACH – New England Automated Clearing House	www.neach.org	New England
PaymentsFirst	www.paymentsfirst.org	Alabama, Georgia, South Carolina and Tennessee
SHAZAM, Inc.	www.shazam.net	
Southern Financial Exchange	www.sfe.org	Alabama, Arkansas, Louisiana, Mississippi, and Tennessee
SWACHA – The Electronic Payments Resource	www.swacha.org	Texas, Louisiana and New Mexico
The Clearing House Payments Authority	www.thepaymentsauthority.org	
Upper Midwest ACH Association	www.umacha.org	Upper Midwest
WACHA – The Premier Payments Resource, Wisconsin Automated Clearing House Association	www.wacha.org	Wisconsin
WesPay – Western Payments Alliance	www.wespay.org	Western states

Health Care

ACH Primer for Healthcare

NACHA — The Electronic Payments Association published an "ACH Primer for Healthcare: A Guide to Understanding EFT Payment Processing" that introduces the healthcare industry to the Automated Clearing House (ACH) Network, explains ACH transaction flow and applications and includes two "next steps checklists," one each for origination and receipt.

https://healthcare.nacha.org/ACHprimer

Healthcare Electronic Funds Transfer (EFT) Standard

This fact sheet, published by the NACHA – The Electronic Payments Association, explains that the Patient Protection and Affordable Care Act (ACA) mandated the identification of a healthcare EFT standard, which was ultimately identified in 45 CFR 162.1602 as NACHA's ACH CCD+ Addenda. Providers can request delivery of claims payments via the healthcare EFT standard and health plans must comply. This fact sheet outlines the benefits of using the healthcare EFT Standard, explains how to enroll to receive the Healthcare EFT Standard, explains what is meant by EFT, and explains characteristics of EFT payment options for healthcare payments including ACH, virtual card and wire transfer.

https://healthcare.nacha.org/sites/healthcare.nacha.org/files/files/NACHA%20HC%20Fact%20Sheet%20-%20Revised.pdf

Webinars

View webinars on the Small Business Payments Toolkit on www.FedPaymentsImprovement.org and YouTube.

"Focus on Payments: What Every Small Business Should Know"
www.youtube.com/watch?v=Hd9J_aK8HeQ

"How to Leverage the Small Business Payments Toolkit"
www.youtube.com/watch?v=rhYSXD3YJYA

"How Financial Institutions Can Leverage the Small Business Payments Toolkit"
www.youtube.com/watch?v=Qh7oGYS5E9c

"How Small Businesses Can Leverage the Small Business Payments Toolkit"
www.youtube.com/watch?v=cFQylqdf8bY