Small Business Payments Toolkit

Remittance Coalition | Volume 2 | 2016

Table of Contents

Introduction

"Small business" is a term applying to organizations of varying sizes and levels of sophistication. We recognize that improving the efficiency of their payments processes is not the primary focus of most small businesses. This toolkit is intended to educate those small businesses that are interested in learning more about payments. The toolkit was produced by 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 term "remittance" refers to details about a payment, such as what the payment is for and variances between the amount billed and amount paid.)

This toolkit is intended to be used by small businesses and the bankers and advisors who serve them in order to encourage the adoption of electronic B2B payments and remittance information exchanges by small businesses. It is the result of collaborative work by a diverse group, including bankers who serve small businesses, business practitioners, software and technology service providers, the Federal Reserve Banks, electronic payments networks and others. We hope you find this to be an informative, helpful resource. 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 remittance.coalition.smb@mpls.frb.org

The Remittance Coalition always welcomes new members and volunteers. To learn more, visit our website at: www.fedpaymentsimprovement.org/payments-efficiency/remittance-coalition/

Note: These materials have been created by the Remittance 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 Remittance 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.

Payment Types Explained

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.

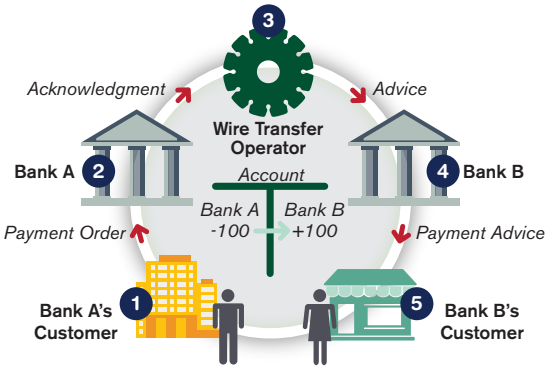
CONS:

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:

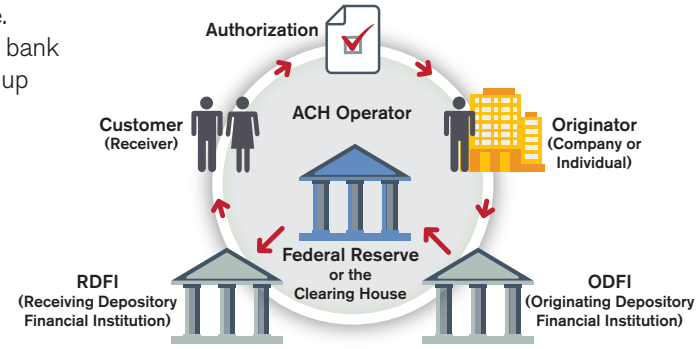
Potentially high cost of acceptance (monthly, equipment and interchange fees). Chargeback amounts and fees are incurred when a customer requests a reversal of a charge for reasons such as claiming fraud, dissatisfaction or non-receipt of service/product.

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.

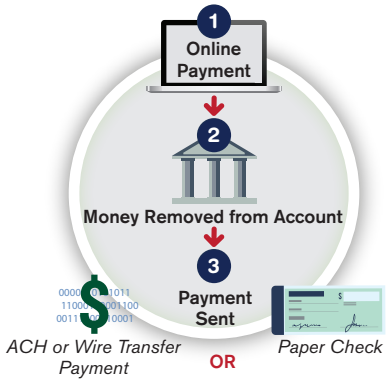
The party originating the transaction must have the receiver's bank routing number, account number and authorization.

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. Provided by either a financial institution or a non-bank provider. Provider sends an ACH payment or check on behalf of 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. 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)

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
- Acceptance is quite widespread among parties being paid, but 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

Understanding ACH

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 11 and "Bankers, Small Businesses and ACH: Getting on the Same Wavelength" starting on page 12.

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)) receives 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 inceptions.
- 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 (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.

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). See description on page 30.
- 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 21.

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. While it may not seem like it, especially in light of the rash of retail data breaches that have been announced recently, paper checks are actually even more vulnerable to fraud. 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 20.

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.

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 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 6-10 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 40 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

Fraud Prevention and Mitigation Tips

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
  - 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 importance of timely reporting on lost, 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 26-27 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
- 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