Published by insideARM LLC
6110 Executive Blvd, Suite 1040, Rockville, Maryland, 20850
editor@insideARM.com | 240.499.3834 | www.insideARM.com

Legal Disclaimer

This information is not intended to be legal advice and may not be used as legal advice. Legal advice must be tailored to the specific circumstances of each case. Every effort has been made to assure this information is up-to-date. It is not intended to be a full and exhaustive explanation of the law in any area, however, nor should it be used to replace the advice of your own legal counsel.

The information and any materials are provided “as is.” insideARM LLC, along with its subsidiary organizations, expressly disclaim all warranties, conditions, representations, indemnities and guarantees whether express or implied, arising by law or custom. In no event will insideARM LLC be held liable for any claim or action arising from or related to your failure to comply with any laws or regulations. Your use of the materials constitutes full and sufficient consideration for, and acceptance by you, of the above terms.

TABLE OF CONTENTS

INTRODUCTION

It's no surprise that everyone who touches a transaction wants to get paid, including the issuing bank, the credit card associations (Visa, MasterCard, etc.), the merchant bank, and the payment processor. At a basic level, every time you process a transaction, you pay several fees:

- **A percent of the transaction amount**: The issuer gets paid by taking a percentage of each sale, called the interchange. This fee varies depending on a bunch of things, such as industry, sale amount, and type of card used. At last check, there were almost 300 different interchange fees!
- **Another percent of the transaction amount**: Your merchant bank takes a cut by charging you a markup fee, the amount here also varies by industry, amount of sale, monthly processing volume, etc.
- **An assessment fee:** The credit card association (Visa, MasterCard, etc.) also charges a fee, called an assessment.
- **A dollar amount for every transaction processed**: The payment processor (who might also be your merchant bank) makes money by charging a fee every time you process a transaction (whether it's a sale, a decline, or return – no matter). Plus, it can charge fees for setup, monthly usage, and even account cancellation.

Usually, the first three fees (the percentages) are all added together and quoted as a single rate, while the transaction fee is quoted separately (e.g., 2.9% + $0.30).

Webinar Playback

Playback of the ARM-U Webinar, **Compliant Payment Cost Reductions**, can be found **here**. The slide deck is included in this workbook at the end of the document.

BENEFITS OF ACH PAYMENTS

Lower Costs

If your business accepts credit and debit card payments, then you're already familiar with the processing fees that accompany these payment methods. But did you know that ACH payments can cost significantly less than credit cards?

When we compare the fees for processing paper checks, credit and debit cards, and ACH payments, credit and debit cards come in at the most expensive, since the fees are typically calculated as a percentage of the transaction. Paper checks have the lowest transaction cost but end up costing merchants more due to time and labor expenses. That leaves ACH payments, which, all things considered, are the least expensive payment method for merchants to accept. When all your transactions are added up, this kind of cost reduction can have impressive effects on your processing fees.

Security

According to the 2016 AFP Payments Fraud and Control Survey, paper checks were the payment method most subjected to fraud in 2014.

It's no wonder that checks are the most vulnerable to fraud—when a customer writes a paper check and sends it through the mail, there are several ways that the check can be compromised or defrauded.

First, the check can be lost, either by the customer or the post office, and may never arrive at the merchant's office. Second, along the way, the check is handled by several different entities and is vulnerable to signature forgery or tampering. The full account and routing numbers and the check-writer's name, phone, and address are all plainly visible on the check, leaving the information susceptible to fraud. And finally, when the check does arrive at the business, the use of paper records and invoices can increase the risk of both fraud and error.

With so many opportunities for fraud or error, it's possible that customers may be reluctant or unwilling to pay via paper check. Fortunately, ACH payments are much more secure than paper checks. For one, ACH payments can't be lost in the mail, and they cut out all intermediaries and reduce the risk of fraud and tampering.

ACH payments eliminate the security risks of paper checks, increasing the chance that your customers will feel safe and do business with your company.

Convenience

ACH payments are convenient for both you and your customers.

Your customers won't have to carry their checkbooks around or send checks in the mail, and they'll have the flexibility of choosing to make a one-time payment or set up recurring billing. And you no longer must deal with trips to the bank or paper invoices, checks, and records—a change that can save you costs on postage, ink, transportation, and labor.

With ACH payments, the funds are transferred electronically, saving you the hassle of dealing with a physical check.

Pros	Cons
Flat rate, low cost ranging between $0.25 - $0.50	Settlements can take up to 5 business days
Priority over paper checks when presented to consumers' checking account	Consumers may not have their routing/account info handy
Paper check conversion reduces risk/potential fraud	Strict rules including limits on returns

ACH Cost Reduction

Since ACH payment solutions are entirely electronic, they require no paper resources, yet enable companies to keep track of finances easily. Because they are also automated, they require no effort to maintain, and no time is wasted in waiting for checks to arrive and then processed.

Companies can benefit from the reliability of the ACH collections system. It ensures money will be automatically taken from the customer's account. It removes the worry for both sides -- consumer and agency -- of remembering to send checks, etc.

ACH transfers are also cheaper to process than other forms of payment.

RISK: ACH payments are good for agencies -- but agencies can find themselves in trouble if scripting gives the impression to consumers that ACH is the only payment type your company will take. All payment options for consumers are on the table, including costly credit/debit options.

WORKAROUND: Lead with the payment option you would like to work with the most.

ACH Quick Facts

- The ACH Network is a batch processing system in which financial institutions accumulate ACH transactions throughout the day for later batch processing.
- Instead of using paper to carry necessary transaction information, such as with checks, ACH Network transactions are transmitted electronically, allowing for faster processing times and cost savings.
- The ACH Network processes two types of transactions: Direct Deposits via ACH and Direct Payments via ACH.
- Direct Deposit via ACH is the deposit of funds for payroll, employee expense reimbursement, government benefits, tax and other refunds, and annuities and interest payments. It includes any ACH credit payment from a business or government to a consumer.
- Direct Payment via ACH is the use of funds to make a payment. Individuals or organizations can make a Direct Payment via ACH as either an ACH credit or ACH debit.
- A Direct Payment processed as an ACH credit pushes funds into an account. An example of this is when a consumer initiates a payment through his/her bank or credit union to pay a bill.
- A Direct Payment processed as an ACH debit pulls funds from an account. An example of this is when a consumer establishes a recurring monthly payment for a mortgage or utility bill, and his/her account is debited automatically.
- ACH credit and ACH debit transactions process quickly. Settlement, or the transfer of funds from one financial institution to another to complete the transaction, generally happens next day.

- Specifically, the NACHA Operating Rules require that ACH credits settle in one to two business days and ACH debits settle on the next business day. Recent enhancements to the NACHA Operating Rules now enable same-day settlement of virtually all ACH transactions.

ACH Fraud

The current form of ACH fraud and account takeover is a combination of social engineering and computer hacking. Where the criminal gains access to a PC either by malware or imposing as someone they are not, and stealing account information and login details so that they can later pretend to be the customer, and make fraudulent ACH transactions, as well as to change notification settings, so that customers are unaware of the transactions until it is too late.

The current breaches that have led to ACH and Wire fraud and corporate account takeover, have all occurred from Origination. This means that, to date, it has been a result of the company or individuals computer completing the ACH transaction having been compromised.

The main risks affecting your computers and ACH transactions are:

- Phishing attacks – use fake email messages from an agency or individual pretending to represent your financial institution. The email may ask you to provide some sensitive information (name, password, account # etc.) and provides links to a counterfeit website. If you follow the link and provide the information, intruders would be able to access your accounts.
    - Phishing attacks may also come in the form of Pop-up windows.
- Vishing attacks – like a phishing attack, except here a person calls you pretending to be a bank representative seeking to verify account information
- Malware/Viruses – computer programs designed to fool you into installing them, the most common of which are pop-ups that try to make you believe your computer has a virus and that you need to download XYZ software to correct the problem. Malware/Virus installations may attempt to complete the following operations:
    - Account information theft (key loggers) – done by capturing keystrokes for your login, and other data used to authenticate your identity.
    - Fake Website substitution – generation of web pages that appear to be legitimate. These man-in-the-middle attacks enable an attacker to intercept your user information, whilst still taking you to the legitimate site.
    - Account hijacking – by hijacking your browser malware can launch a hidden browser window on your PC, which is then used to access your accounts.
- Pharming – typically sent in an email attachment or link within an email. These emails are usually sent to large groups of recipients, and usually contain numerous grammatical and spelling mistakes.
- Social Engineering – social engineering attacks occur in many forms, but typically are directed at a specific individual or company. The attacker attempts to gain as much information as possible via the user's social network, and or by fooling individuals into

providing information that can be used to gain access to bank accounts, or other sensitive information.

Suggested Fixes:

- All ACH customers undergo a full credit evaluation and electronic payment risk analysis.
- Use of Tokens by Originators
- Set Exposure limits for each customer
- Active monitoring of exposure limits by dedicated staff
- Annual review of exposure limits Continuous staff education as to NACHA Operating rules governing ACH transactions
- Formal process for requests regarding change of address

Webinar Q&A

What is a targeted NSF rate you look for?

Unauthorized = .5%

Additional returns = 3%

Overall = > 15%

Any suggestions for scripting to take recurring ACH payments over the telephone?

The important thing to remember is that the consumer, ultimately, has the power to decide what payment method they'll use. It's also important to keep in mind you must include free payment methods to consumers – methods that don't tack on a service fee.

You can script your ACH request by mentioning that first: "We accept payments via ACH, paper check, etc." You're relying on people to go with the first option; it makes sense that your first option will be the one that is the lowest cost to you.

How are agencies using Venmo? Is the consumer paying via the app or are they required to go to State's portal to use Venmo.

Venmo is a mobile payment service owned by PayPal. It allows users to transfer money to others using the service via a mobile phone app. Both the sender and receiver have to live in the U.S. Venmo is a type of payment rail.

Some agencies are exploring using Venmo (or other cash-sharing/sending mobile apps) as a way to receive payments from consumers. How best to incorporate Venmo into your payment processing strategy is a great conversation that should include your IT department, your compliance team, and your general counsel.

Are there any regulations or laws that need to be followed to auto-update credit cards that have expired?

If a consumer agrees to automatic payments, they can continue even when the card expires. Vendors and other entities can obtain your new credit card number through a card updater service offered by your credit card issuer. These services provide merchants with new information for customers whose accounts have new credit card numbers or updated expiration dates. American Express, MasterCard, Visa and Discover all offer such services.

Where we are seeing risk is when consumers aren't aware that their credit cards have an "auto-renewal" feature that updates the number or expiration date for merchants who have the card details on file.

You'd be well-served reading about **Restore Online Shopper's Confidence Act, or ROSCA**. Per the FTC's website, "This Act prohibits any post-transaction third party seller (a seller who markets goods or services online through an initial merchant after a consumer has initiated a transaction with that merchant) from charging any financial account in an Internet transaction unless it has disclosed clearly all material terms of the transaction and obtained the consumer's express informed consent to the charge. The seller must obtain the number of the account to be charged directly from the consumer."

Discuss with your own legal counsel, but it may be a smart move to make explicit in your payment terms and conditions that debit/credit cards will auto-update, and lay out clear ways for consumers to discontinue their auto-payments.

Webinar Slide Deck