Combating Same Day ACH Wire Fraud

Using Transaction Monitoring, Multi-Factor Authentication, and Behavioral Analytics

VASCO®

TRUST FOR THE DIGITAL WORLD

Table of Contents

ACH payments as an alternative to paper checks

ACH payments are electronic payments made through the Automated Clearing House (ACH) Network. The Automated Clearing House is an electronic network that allows you to make payments or collect funds electronically through the ACH network by directly debiting/crediting the customer's checking or savings account.

The most common uses of ACH are online bill payment, mortgage and loan repayment, and direct deposit of payroll. These payments are an efficient and cost-reducing alternative to paper checks and credit cards.

How do ACH payments work?

Only banks can initiate ACH transactions. Therefore, businesses and merchants need to partner with banks in order to set up ACH payments. The merchant or company setting up the transaction is known as the originator; the partner bank is referred to as the Originating Depository Financial Institution or ODFI. The customer's bank would be the Receiving Depository Financial Institution or RDFI. The ODFI and RDFI are responsible for verifying that the accounts exist, ensuring that the funds are available and that the transaction complies with the International ACH Transaction rules issued by NACHA.

To execute an ACH payment, two things are required: authorization and a routing number. Firstly, a customer gives an originating institution or corporation the authorization to debit the amount due directly from their checking or savings account. Secondly, the customer needs to enter an account and routing number. An Automated Clearing House routing number is a nine-digit number that is assigned for electronic transactions between financial institutions. This number is unique to banks and its branch offices and identifies the clearing house.

Only banks can initiate ACH transactions. Therefore, businesses and merchants need to partner with banks in order to set up ACH payments. The merchant or company setting up the transaction is known as the originator; the partner bank is referred to as the Originating Depository Financial Institution or ODFI. The customer's bank would be the Receiving Depository Financial Institution or RDFI. The ODFI and RDFI are responsible for verifying that the accounts exist, ensuring that the funds are available and that the transaction complies with the International ACH Transaction rules issued by NACHA.

To execute an ACH payment, two things are required: authorization and a routing number. Firstly, a customer gives an originating institution or corporation the authorization to debit the amount due directly from their checking or savings account. Secondly, the customer needs to enter an account and routing number. An Automated Clearing House routing number is a nine-digit number that is assigned for electronic transactions between financial institutions. This number is unique to banks and its branch offices and identifies the clearing house.

An example: In order to establish direct deposit of your paycheck, you provide your routing and account number to your employer. Your employer's ACH processor initiates the funds transfer to your bank account using the ACH network. Similarly, to debit your bank account for the purpose of bill payment (e.g. your electricity bill), your utility company sends an ACH debit entry to its ODFI. The ODFI and RDFI ensure that the funds are available in your bank account and then process the transaction so that the funds are sent to the utility company's bank account.

In most cases there isn't a limit on how much money can be paid at one time and ACH transactions are often processed in bulk (for example, paying all your employees on one date). These bulk transactions appeal to hackers seeking to gain the largest possible payouts if they are successful in intercepting them. In the US, ACH fraud is a huge problem.

What Is ACH Fraud?

ACH fraud is the theft of funds through the Automated Clearing House financial transaction network. The ACH network acts as the central clearing facility for all Electronic Fund Transfer (EFT) transactions in the United States. [1] Although ACH and wire transfers can be for any amount, ACH transactions generally include online bill payments and other scheduled transfers of smaller amounts of money, while wire transfers can involve larger sums transferred between domestic and international banks. [2]

ACH fraud often goes unreported or under reported. In fact, many banks often categorize it as account takeover or online banking fraud. With the advent of Same Day ACH payments, where payments are settled in hours instead of one or more business days, hackers are increasingly taking advantage of these shorter payment windows by sneaking in fraudulent transfers. [3]

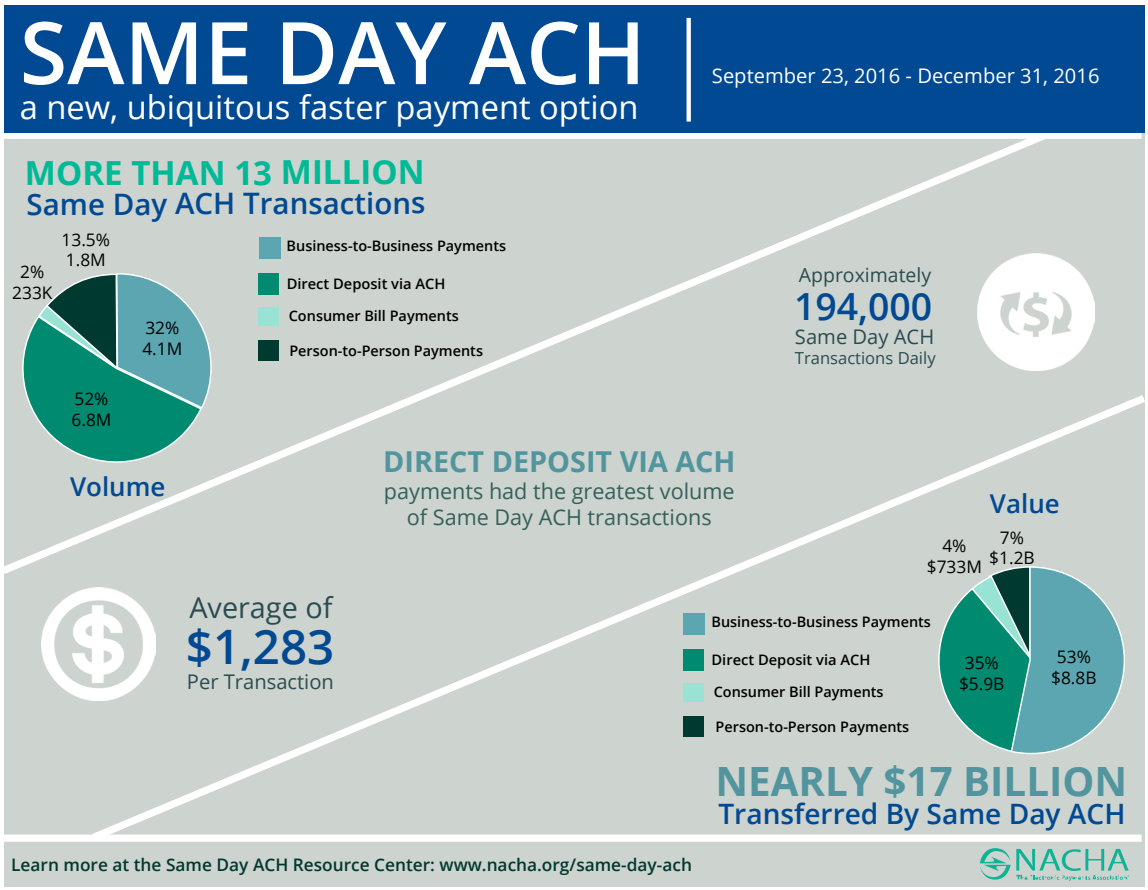
Unlike retail banking, corporate banking, including ACH, is not federally insured or protected. This means that if an attack were to occur and an organization was to lose money, there is no recourse to recover that money. While the bank may try to recover the money, it is under no obligation to do so. In fact, in most situations, if an ACH fraud is not caught early enough, the money is lost forever.

> “ ACH fraud is the theft of funds through the central clearing facility for all Electronic Fund Transfer transactions in the United States. ”

By The Numbers

In April 2017 NACHA reported that the aggregate dollar volume of payments over the ACH Network in 2016 totaled $43.7 trillion, (or 25 billion payments), a 5.1% increase over 2015. [4]

Between the Same Day ACH initiative launch on September 23, 2016 and December 31, 2016, there were more than 13 million same-day ACH transactions, reflecting nearly $17 billion:[5]



Examples of ACH attacks

Prior to same-day settlement of processing and settlement of virtually any ACH payment, examples of ACH wire fraud included:

- A fraudster gains access to a commercial customer's credentials, generating an ACH file in that customer's name and withdraws funds before the customer discovers the theft.

- A fraudster gains access to a retail customer's credentials and then assumes their identity by setting themselves up as an automatic bill pay recipient.

- An insider (an employee of the target company) modifies ACH files to steal funds.

- A fraudster using classic check kiting, a scam in which funds are juggled between bank accounts at separate banks, takes advantage of the time lag in transactions to settle accounts.

- As part of a spear phishing scam, an employee authorized for ACH transactions receives an email directing him to an infected site. In turn, they unknowingly install a keylogger to access authentication information. Once they have access to the account, the criminals create ACH payments to new recipients, often accounts belonging to money mules paid by the criminals, who then, as instructed, transfer the illicit funds overseas or withdraw the money. To ensure their fraudulent ACH payments go undetected, criminals may change the compromised account's contact information. If the bank attempts to contact their customer about an abnormal ACH payment, they are actually contacting someone within the criminal's network, who can then confirm the "validity" of the payment. As a result, the fraudster can then impersonate the company's ACH-authorized employee and withdraw funds.[6]

- In a variation of a Man-in-the-Middle attack, hackers use malware to gain access to a corporate email account and then monitor the victim company's payment requests and other communications. Posing as a trusted vendor, the cyber-criminals send a request for payment, instructing the company to wire the money to a bank account that appears to be legitimate, but is really under control of criminals. By the time the fraud has been discovered, the money has often been collected and the thieves have disappeared.

- With Vendor Impersonation Fraud (VIF), a fraudster will contact a business, impersonating a legitimate vendor or contractor. This information is often publicly available, especially when it comes to public sector companies. In most instances, they will request the update of their account information, providing a new account number and routing information. When the next invoice from the vendor is paid, the funds, instead of being sent on to the authorized vendor, wind up in the fraudster's account. [7]

How Same Day ACH Changes the Kinds of Fraud Banks Encounter

From online and corporate account takeovers to batch file manipulation, sleeper fraud and more, here are five types of fraud most impacted by same day ACH: [8]

Online Banking Losses Increase

Account takeover is a $5 billion (and growing) problem. In 2016, the Auriemma Group reported nearly a 300% increase in account takeover, mostly due to consumers who repurpose their same login credentials across all of their online sites. [9]

As a result, fraudsters trolling the Dark Web have used brute forces attacks, such as credential stuffing, to take over their online banking accounts. Even if one of these credentialing attacks fail, there are literally hundreds of thousands more to try and with hundreds of bank sites available, they can test each one out until they find one that works. Once that happens, the fraudster can quickly drain a customer's account(s) by moving from those accounts to theirs, in much the same way as they do through social engineering schemes.

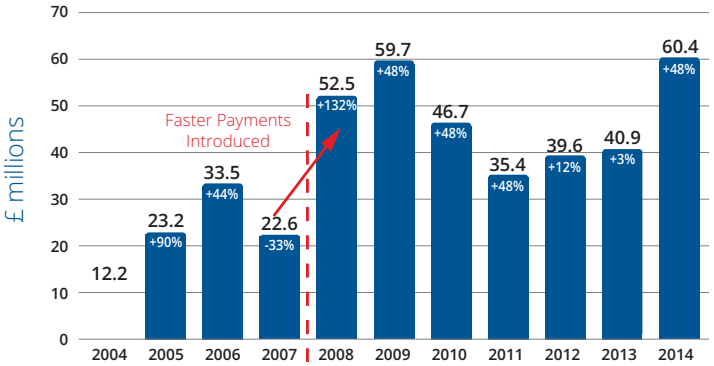
Additionally, although the outcomes may ultimately differ slightly, it is useful to consider what happened in the UK when it launched faster payments. It turns out online banking losses doubled immediately after Faster Payments launched and have since never come back down to the pre-faster pay levels. [10]

Corporate Account Takeovers Increase

FBI documents show there were over 22,000 cases of fraudulent transfers totaling approximately $3.1 billion between October 2013 and May 2016. According to Trend Micro, organizations victimized by a Business email compromise lost an average of $140,000 per attack, with the highest number of attacks occurring in the U.S. (11)

None of this is especially surprising as business and corporate deposit accounts can result in million dollar paydays while personal accounts may only gain the fraudsters a few thousand dollars. In the case of corporate accounts there is also the matter of insider theft by employees including payroll fraud, account to account fraud schemes, payments made to fictitious vendors as well as embezzlement.

Online Banking Fraud losses 2004 - 2014



Batch ACH File Manipulation Expands

Like other B2B transactions, including payroll files, insurance claim payments, or bill pay transactions, ACH files are submitted in batches. In the case of ACH batch files, there are three ways in which files can be manipulated or initiated. These include:

Fraudster Creates a Fraud Payroll Batch File. Fraudsters, who have previously gained access to the corporate accounts bank, submit a bogus payroll file that looks similar enough to legitimate files so it doesn't raise red flags.

Fraudster Changes a Few Records within a legitimate Batch File. To reduce their chances of being detected, fraudsters might change select records within a legitimate batch, such as adding new employee paychecks.

Fraudster Changes Payee Account Numbers. In this instance the fraudster only changes a single detail, such as the payee account number where the funds are to be routed.

These batch attacks can be performed readily because a number of banks fail to put in the basic security measures, such as using what is known as "Dual Approvers".

In fact, it is still common to see banks that allow corporations to submit ACH batches with only a single user name and static password. This account is then easily open to phishing attacks that anticipate a chain reaction of increasingly sophisticated attacks and alternating defensive/mitigation responses.

The impact on banks of this kind of batch manipulation can result in significant losses; however, when banks have strong front-end authentication controls coupled with monitoring tools to flag suspicious batches or transaction, the impact can also just as quickly be reduced.

Money Mule Stockpiling & Sleeper Fraud Become Prevalent

Money Mules and their accounts are used to receive fraudulent ACH or Wire payments so that the money can be disguised and paid to fraudsters. This includes everything from deposit accounts, credit card accounts or any other kind of account capable of receiving ACH payments. Often, the debiting as well as the receiving ACH account has been taken over. As a result, money mules may or may not be aware of how they fit into the fraud scheme

On the other hand, Sleeper Fraud involves the stockpiling of money mule accounts for later use in a fraud scheme. By having access to multiple accounts, fraudsters can quickly monetize their fraud schemes to steal potentially millions from banks very quickly. As a result, banks should be aware that the risk of fraud is associated with not only the debiting but also of the receiving of ACH transactions.

Payment Fraud and Bill Pay Losses Rise

Same Day ACH also has implications for those banks that track their ACH and Bill Pay Fraud losses. Fraudsters can set up new payees and send funds, or even divert them to new locations using the same payee accounts and changing the details. As a result, Bill Pay losses will likely increase in the wake of same-day ACH.

How Banks Can Mitigate Same-Day ACH Risks

So how can you protect your bank or financial institution against classic, as well as, same-day ACH/wire fraud? Among analysts and third-party payment processors the consensus is that a layered security approach — using technologies to authenticate the user, using analytics to understand customer and criminal behavior, and leveraging out-of-band technologies where appropriate or based on the level of risk the transaction presents — reduces fraud. Additionally, having a single view of the customer, supplying insight by the institution to understand short-term behavior across the transaction channels they routinely use and how that behavior changes when it comes to channels such as mobile banking, is equally critical. [12]

A layered, adaptive and integrated security payment initiative provides the following capabilities:

- **Strong, multi-factor authentication** for senders who initiate transactions and for those sending files to the receiving bank. This includes originating banks requiring robust authentication of senders who initiate transactions, as well as strong security for files sent to the receiving bank
- **Behavioral analytics** to provide risk scoring and, based on level of risk, dynamically utilize step-up authentication to validate the user
- **e-Signatures** to digitally automate and manage document-based transactions that require signatures, approvals, and forms/data capture
- **Machine Learning** dramatically simplifies the fraud scoring of vast data that leverage sophisticated analysis of behavioral, contextual and other key data elements that ultimately drives instant action when fraud patterns are identified
- **Transaction monitoring** for detecting fraudulent activity. Transaction data such as the date and time requested, the payee account and name, the account number and the method used to initiate the ACH are captured.

VASCO Solutions to Combat ACH Wire Fraud

VASCO offers a number of key solutions to help your bank's digital transformation and to combat ACH Wire Fraud. Our solutions, based on years of working with banks, have been tested and proven to mitigate these risks. Here are the steps we recommend:

Step 1: Implement Dual Approvers within your ACH application and enforce two-factor authentication on both the Requestor and Approver.

Having just a single user, even for small businesses, opens a large security hole in ACH systems. If approvers and requestors are only using a strong password, it's nearly equivalent to not having a solution in place at all.

To supplement strong passwords, VASCO recommends organizations implement two-factor authentication, at the very least One Time Passwords (OTPs) or PUSH-enabled One Time Passwords. However, One Time Passwords are not the same as Two-Factor authentication; instead, they must be used with either a PIN at the login screen or on the device or biometrics on the device. DIGIPASS for Mobile makes it easy to implement Two-Factor Authentication with native support for both Fingerprint and Facial Recognition biometrics and reduces end-user friction.

Step 2: Perform real time analytics on your transactions

With Same-Day ACH, transactions happen quickly and your systems and processes need to keep up. Implementing a Real-Time Risk Analytics system, such as VASCO's IDENTIKEY Risk Manager, which uses Artificial Intelligence and Machine Learning, helps prevent potentially fraudulent transactions. In the past, transactions were flagged for Security Risk Teams to analyze and make decisions on how to handle. Today, AI and machine learning help to simplify these processes by analyzing all transactions and comparing vast data to create an accurate view of fraud in real-time.

IDENTIKEY Risk Manager combined with DIGIPASS for Apps ensures not only the most comprehensive, real-time fraud detection and prevention by utilizing vast client-side data points within the risk analysis engine; it also provides enhanced data protection thanks to Secure Channel encryption (i.e. Communication between client and server) and application shielding.

Step 3: Electronically sign your documents

By leveraging e-signatures technology, you ensure that your customers can complete document-based transactions anytime, anywhere and on any device. VASCO's eSignLive e-signature solution is built on over two decades of best-in-class signing, authentication and workflow capabilities, which balance ease-of-use with the highest levels of security and compliance.

Designed for the unique requirements of our banking clients, the solution enables banks to automate and digitize their key document-based business processes. Moreover, eSignLive's patented audit trails make it faster and less costly to prove compliance and deflect legal disputes by gathering electronic evidence of exactly what transpired during the transaction. In addition, transactional data collected throughout the signing experience can be used to validate the integrity of the process, as well as pinpoint areas of drop-off or confusion to further optimize the customer experience.

With eSignLive, banks spend less time managing paper-based. The entire transaction process can be completed in one session, in any channel (e.g., in-branch, online, mobile) and is interoperable with both upstream (e.g., document generation, eForms, BPM, etc.) and downsteam systems (e.g., ECM, records management, storage, e-vaulting, etc.).

Step 4: Create a full end-to-end trusted environment for processing your transactions

Transactions that take place in the digital world are fraught with risk including fraudulent behavior and cyberattacks that can compromise your business, your operations and your customers. That's why maintaining trust across your digital processes is extremely important.

VASCO's Trusted Identity Platform allows you to take the ACH process and easily digitize the related security. It does this by building the trust between the bank and the mobile application, and likewise between the mobile application and the user. With a full end-to-end trusted environment, the bank can roll out new services and features faster while maintaining the right level of security at all times.

SOURCES

1. whatis.techtarget.com/definition/Automated-Clearing-House-fraud-ACH-fraud
2. www.cnb.com/fraud/ach-wire.asp
3. www.verteks.com/2017/05/wire-transfer-scams-cost-average-140000-per-attack
4. verafin.com/2017/06/ach-payments-mitigating-risks-faster-fraud
5. www.pymnts.com/news/faster-payments/2017/nacha-releases-first-same-day-ach-stats
6. verafin.com/2017/06/ach-payments-mitigating-risks-faster-fraud
7. verafin.com/2017/06/ach-payments-mitigating-risks-faster-fraud
8. frankonfraud.com/fraud-trends/5-fraud-schemes-that-will-probably-hurt-you-with-same-day-ach
9. salduttilaw.com/6928-2
10. rankonfraud.com/fraud-trends/5-fraud-schemes-that-will-probably-hurt-you-with-same-day-ach
11. www.verteks.com/2017/05/wire-transfer-scams-cost-average-140000-per-attack
12. www.fico.com/en/blogs/fraud-security/the-growth-and-evolution-of-achwire-fraud
13. www.vasco.com/products/application-security/digipass-for-apps.html
14. www.vasco.com/products/management-platforms/identikey-risk-manager.html
15. www.esignlive.com

About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit blog.vasco.com

VASCO®

TRUST FOR THE DIGITAL WORLD