» 2020 Report

As payment card security rises, ACH fraud grows

MARQETA

Advances in payment card security are challenging long-held assumptions about the most secure way to pay

Electronic payments sent through the automated clearing house (ACH) system have long been perceived as a safer form of payment than checks, which can be intercepted with relative ease, or payment cards, which can be cloned, counterfeited, or stolen in a data breach. For decades, this impression was backed up by data. As ACH transfers grew to become the dominant form of payment in the United States — with network payments reaching $41.6 trillion in 2015 — the rate of ACH fraud was stable at .0008% of payment value, the lowest of all payment types.[1]

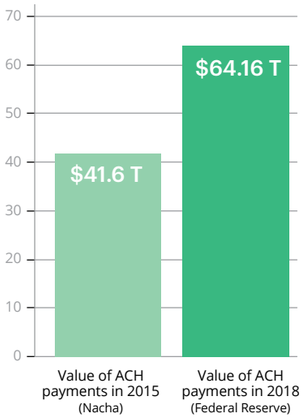
But ACH's status as a more secure way to pay is being challenged by the widespread adoption of EMV chip cards and virtual cards, as well as the increased use of dynamic spend controls and tokenization. These advances in payment card security are proving to be effective. In 2018, ACH was the only payment method to record an increase in fraud rates, according to the Association for Financial Professionals' Payments Fraud and Control Survey.[2] That year, the percent of organizations experiencing fraud via ACH credit transfers increased to 20%, up from 7% during the prior year, and the percent of organizations experiencing fraud via ACH debit transfers rose to 33%, up from 28% in 2017.[3]»

"In 2018, ACH was the only payment method to record an increase in fraud rates."

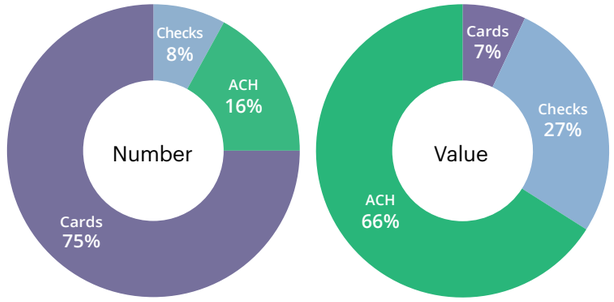
Source: Association for Financial Professionals' "Payments Fraud and Control Survey"

ACH transfers offer fraudsters an attractive target

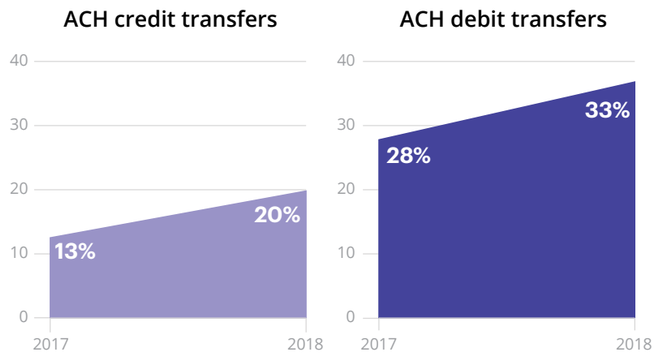
ACH is the dominant form of payment in the U.S. by value*



Share of payments by number and value*



A growing number of organizations are experiencing fraud via ACH debit and credit transfers*



Sources: Nacha, "ACH Volume Grows by 5.6 Percent Adding 1.3 Billion Payments in 2015," April 14, 2016; *The 2019 Federal Reserve Payments Study*; and "Association for Financial Professionals," *2019 AFP Payments Fraud and Control Survey Report*

An account number and a routing number

As advances in payment card security become broadly available through modern card issuing platforms like Marqeta, ACH transfers are looking increasingly attractive to fraudsters. In terms of value, the average ACH credit or debit transaction dwarfs the average payment card transaction. In 2018, the average amount of an ACH credit transfer was $3,434.45, the average amount of an ACH debit transfer was $1,402.41, and the average amount of a payment card transaction was $53.96. Banks do not always actively monitor ACH transfers for fraud, and even when they do, checking accounts for unusual activity typically involves a combination of customer detection and automated and manual bank processes. According to KPMG's recent Global Banking Fraud Survey, 89% of financial institutions said they relied on customers to bring fraud to their attention, compared to 82% who relied on automated systems, and 71% who relied on manual systems.[4]

Customer awareness of payment card fraud is high — about 42% of consumers in the United States and the United Kingdom have experienced a fraudulent transaction made in their name. In contrast, ACH payments, which are typically orchestrated directly by financial institutions, are viewed as a more trusted way to pay. The ease with which the ACH payment network can be compromised has come as a surprise to victims.[5]

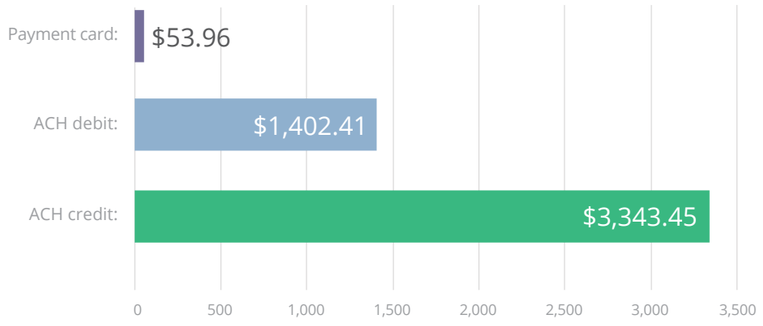
"The thief or thieves who got us needed just two elements: our company's bank account number and routing number," recalled JJ Hornblass, CEO of Royal Media, which had nearly $50,000 siphoned out of its bank account over a matter of days. "Those elements are prominently displayed on every paper check and required for inbound wire transfers. It is nearly impossible to ensure those numbers are kept safe from criminals."[6]

According to the FBI, small- to medium-sized businesses, in particular, have suffered attacks by ACH fraudsters in the past. "In most cases, the victims' accounts are held at local community banks and credit unions, some of which use third-party service providers to process ACH transactions," said Alan P. Peak, special agent for the FBI Kansas City Division, in a presentation on financial fraud given in 2009.[7]

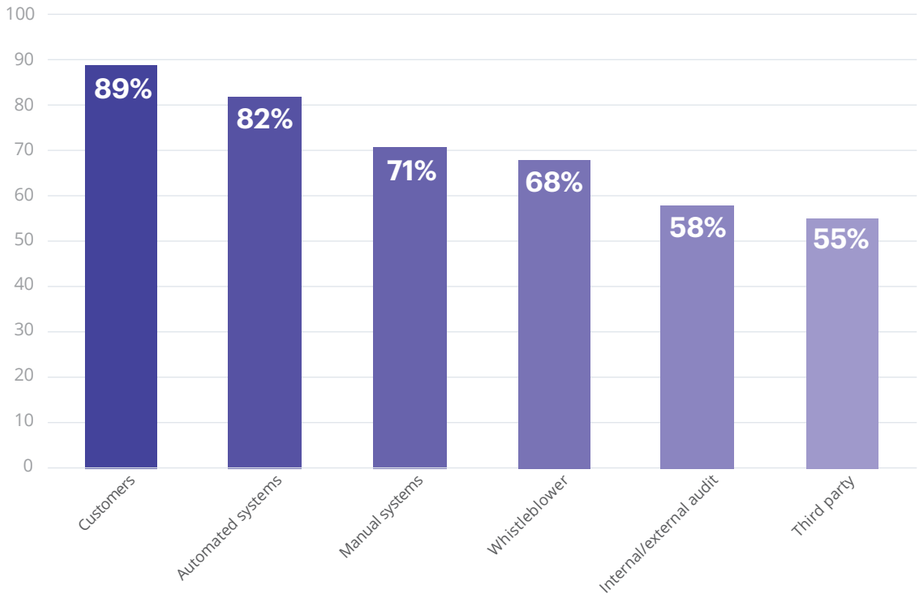
More recently, individuals have been targeted. Venmo, the mobile payment service provider owned by PayPal, has an article on its website informing people what to do if they see charges on their bank statement from Venmo if they don't have a Venmo account. "If you confirm the payments were not authorized by you or someone with permission to use your card, it's likely someone has gained unauthorized access to your personal and/or financial information," the article warns. Venmo recommends updating passwords and requesting a new account number, among other steps.[8]

ACH transfers are bigger and less protected than card payments

Average payment amount by payment type**



Banks rely on customers as their #1 fraud detection method**



***Sources: The 2019 Federal Reserve Payments Study* and KPMG International, *Global Banking Fraud Survey,* 2019

Faster and more vulnerable to fraud

A worldwide push for faster payments led in the United States by the Federal Reserve — could make ACH transfers more vulnerable. As transaction times shrink without a corresponding reduction in the time it takes to detect fraud, fraudsters gain an advantage.

Dwolla, which offers an API to facilitate payments using same-day ACH, mitigates the risk of a requested return (as would occur in the case of a fraudulent payment) by waiting three or four days to make standard ACH debits available. However, in a December 2019 article, "The Waiting is the Hardest Part: How Long do ACH Transfers Take," Dwolla acknowledged that some customers want their money faster. "As transactions speeds increase, so does the risk for each transaction," Dwolla warned.[9]

Federal law protects consumer account holders from unauthorized ACH transfers, provided they notify their financial institution within 60 days of learning of the fraudulent transfer from their bank statements. But commercial account holders have much less time to act. According to Bondi Iovino & Fusco, a law firm based in New York's Nassau County, commercial claims can be dismissed after 24 hours. Unlike consumer accounts, which are protected by Federal Reserve Regulation E, commercial accounts are classified under the Uniform Commercial Code and governed by bank policies. Bondi Iovino & Fusco recommend using payment cards instead of checks for business expenses. Not only do payment cards offer superior protection in the event of a theft, but checks can expose a business to ACH fraud. "Anyone who has a check from your business has all the information needed to steal money from your account via a fraudulent ACH transfer," Bondi Iovino & Fusco warned in a blog post on their website.[10]

According to Nacha, the steward of the ACH network in the United States, the use of same-day ACH during the first three quarters of 2019 increased 41% over the same period in 2018. Approximately 250 million same-day ACH payments were made in 2019, according to the organization. The limit for same-day ACH payments rose from $25,000 to $100,000 on March 20, 2020.

The move to same-day ACH gives fraudsters an advantage

Companies have less protection than consumers[+]

24 hours
the window some banks give business customer to report a fraudulent transaction

60 days
the window a consumer has to report a fraudulent transaction under federal law

The use of same-day ACH payments is on the rise[+]

41%
the increase in same-day ACH payments during the first three quarters of 2019 compared to the same period during the prior year

250 million
the number of same-day ACH payments in 2019

$100,000
the maximum amount of an ACH payment

[+]*Sources:* Bondi Iovino & Fusco and Nacha

Falling fraud rates, and a decrease in losses

The intensification of attacks on the ACH network has been accompanied by a steep decline in counterfeit card fraud and a smaller decrease in the rate of payment card fraud overall. According to Visa, merchants reported a 76% drop in losses from counterfeit fraud after upgrading their POS systems to accept EMV chip cards at the request of the card networks. In contrast to standard magnetic stripe cards, which are printed with both primary account numbers (PANs) and card verification values, EMV chip cards dynamically create a new transaction code each time they are used. This code is then encrypted and provided to a merchant at the point of sale along with the PAN, rendering the cards very difficult to counterfeit.[11]

EMV chip cards have been less effective in preventing card-not-present fraud that occurs when cards are used online. Card-not-present fraud has surged in the double digits since network rules requiring merchants to accept EMV chip cards took effect in 2015. But as other security measures such as dynamic spend controls, virtual cards, and tokenization take hold, online fraud is also coming under control. According to *The Nilson Report*, card fraud peaked worldwide in 2016 at 7.15 cents per $100 of transaction volume. This year, global card fraud is estimated to decrease to 6.83 cents per $100 of transaction volume.

Dynamic spend controls limit the conditions under which a payment can be made. When cards are created on modern card issuing platforms like Marqeta, dynamic spend controls set by the card program manager programmatically restrict payments by merchant, merchant category code, amount, country, frequency of use, start/end dates or times, and many other variables. Virtual payment cards, which like plastic cards are identified by a 16-digital PAN, can be created for a single transaction, eliminating the possibility that a card can be reused by a fraudster.

Tokenization adds still another layer of security to modern payment cards. Tokenization replaces the PAN displayed on the front of a payment card with surrogate data. Typically used in conjunction with a digital wallet, tokenization affords advanced protection to traditional plastic payment cards and virtual cards. Instead of receiving a PAN and storing it in a database that can later be compromised by fraudsters, merchants receive a token and a dynamically generated transaction code. This eliminates the risk that a customer's payment information will be compromised in a data breach, and it also protects customers in the event that the device storing their digital wallets is lost or stolen.

The combination of dynamic spend controls, virtual cards, and tokenization has led to fraud rates that can be as much as ten times lower for payment cards created on a modern card issuing platform than for traditional payment cards.[12]

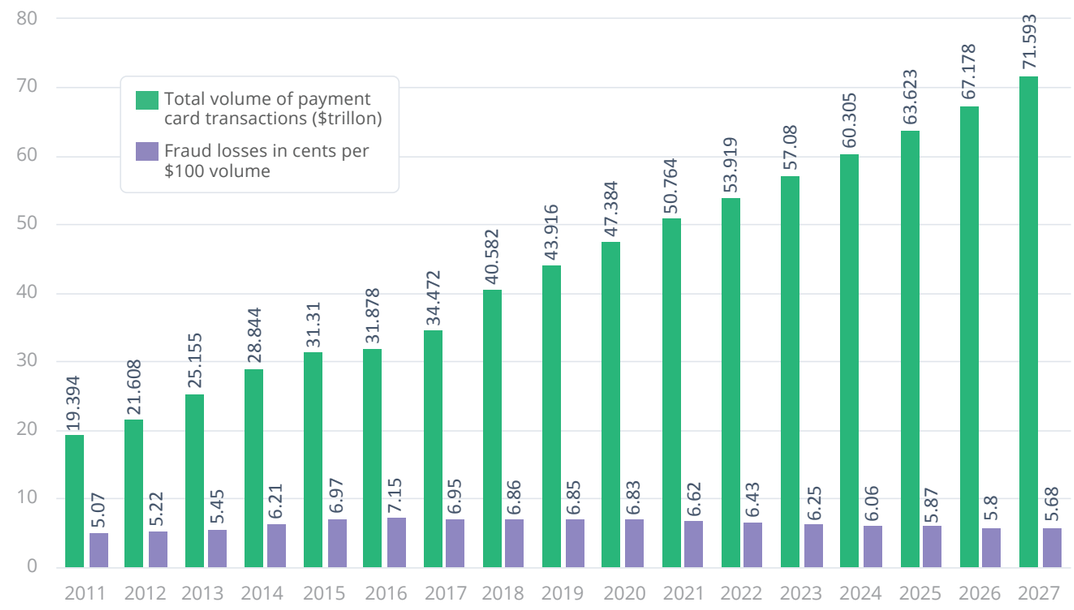
A steep decline in fraud losses

Counterfeit fraud plunged as use of EMV chip cards spread[++]

7.15¢
Card fraud peaked at 7.15¢ per $100 in sales volume in 2016

76%
decline in losses from counterfeit fraud

Payment card fraud rates are falling around the world, as volume rises[++]



[++]*Sources:* Visa and *The Nilson Report*

Final thoughts:

The theory put forward by criminologists that opportunity is a root cause of crime is supported by a significant change in the pattern of payment-related crime over the last five years. In 2015, an increase in payment card security brought about by a new requirement to accept EMV chip cards at point-of-sale terminals dramatically reduced the opportunity for traditional forms of payment card fraud. Fraudsters were denied easy access to the primary account numbers, or PANS, at the point of sale, making it more difficult to create counterfeit cards. At the same time, the rise of modern card issuing and processing led to increased use of dynamic spend controls, one-time-use virtual cards, and tokenization — all of which make it harder to steal PANs from online data stores and, also, harder to misuse that information if it was obtained.

Compared to payment cards, some fraudsters saw a greater opportunity in ACH fraud. All a payment thief needed to create a fraudulent ACH transfer was an account number and a routing number, which could be easily obtained from a check or by calling a bank. As payment card fraud rates decreased, ACH fraud rates increased. The average ACH payment was larger than the average card payment, and ACH transfers were typically not monitored as closely as card payments. This trend will likely continue barring any major change in the dynamics of the payment industry. The rate of ACH fraud is set to increase as long as the opportunity to commit ACH fraud is perceived to be elevated in relation to payment cards.

SOURCES

1: Nacha, "ACH Volume Grows by 5.6 Percent Adding 1.3 Billion Payments in 2015," April 14, 2016 and Federal Reserve, "Changes in U.S. Payments Fraud from 2012 to 2016," October 2018
2: Association for Financial Professionals, "2019 AFP Payments Fraud and Control Survey Report"
3: Ibid
4: Federal Reserve, "The 2019 Federal Reserve Payments Study" and KPMG International, "Global Banking Survey 2019," p. 14
5: Marqeta survey of cardholders in the United States and the United Kingdom, January 2020
6: *Bank innovation*, "ACH Is a Sieve of Fraud That Needs to Be Fixed," February 26, 2018
7: FBI, "Fraudulent Automated Clearing House (ACH) Transfers Connected to Malware and Work-at-Home Scams," November 3, 2009
8: Venmo articles
9: Dwolla, "The Waiting is the Hardest Part: How Long Do ACH Transfers Take?" by Joey Aguirre, December 6, 2019 and Dwolla, "Understanding the ACH Returns Process," by Lindsey Richardson, April 1, 2020
10: Bondi Iovino & Fusco, "What Can Business Owners do to Prevent Loss from ACH Bank Fraud?" June 22, 2016
11: Visa, "Chip technology helps reduce counterfeit fraud by 76%," May 28, 2019
12: Federal Reserve and Marqeta Research

MARQETA

About Marqeta

Marqeta brings speed and efficiency to card issuing and payment processing with the world's first open API platform. Businesses have been limited by slow legacy platforms that did not allow for flexible new program set up and fraud control. Marqeta's platform allows customers to instantly issue cards with much-needed flexibility, control, and scale. Our modern platform was built from the ground up, and our APIs power innovative payment experiences for many of the apps and services you enjoy daily. Highly configurable, secure, and reliable, Marqeta's platform helps B2B and B2B2C companies compete in a constantly changing digital world.

Today Marqeta has 350+ employees and operates globally in the U.S., U.K., E.U., Canada, and the Asia-Pacific region. We have extensive partnerships with multiple banks and card networks, including Visa, Mastercard, and Discover. Our customizable solutions are used by innovators in areas such as expense and supplier management, digital banking, lending, e-commerce, on-demand services, and disbursements and incentives.

Marqeta is backed by leading global investors including Visa, Iconiq, Goldman Sachs, and Coatue Management. In May 2019, we raised a Series E of $260 million, raising the value of Marqeta to nearly $2 billion.