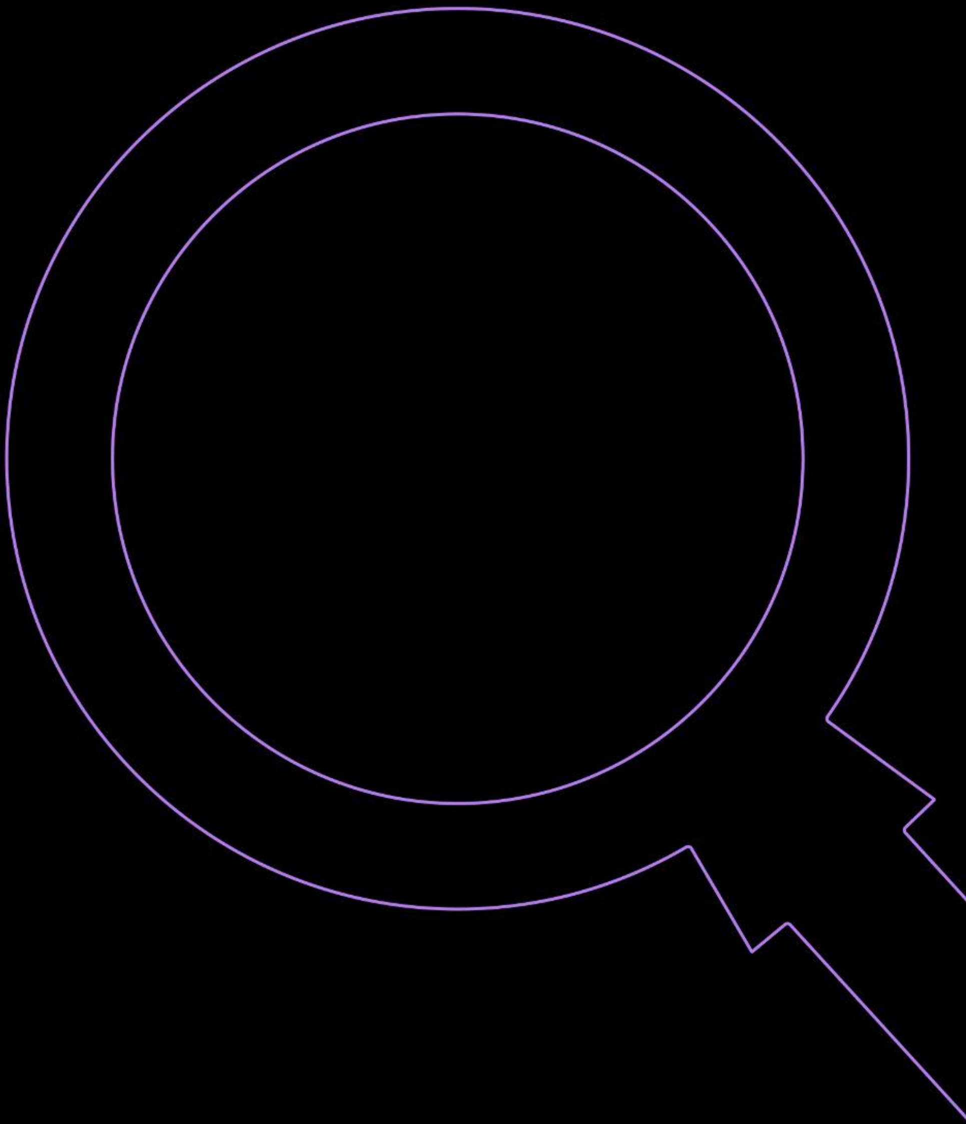
BLOCK



December 2024

How Cash App Is Fighting Scams

Introduction

The financial technology landscape has changed dramatically, and today people have access to more financial tools than ever before. These technologies have brought new financial use cases and opportunities to millions of people, who can now manage, spend and send their money across literally thousands of platforms, both online and offline.

Of course, with each wave of financial innovation comes a new set of challenges. While scams are not new, the rise in digital activity with phones, emails, internet, communication platforms, and especially social media, has fueled the prevalence of scams. And scammers have become increasingly adept at identifying, engaging, and exploiting their victims with sophisticated tactics.

This white paper examines the growing complexity of scams, and how companies like Block are proactively addressing the emerging risks as the financial ecosystem continues to evolve. Building a united front against scams means fostering collaboration across industries and sectors—government, law enforcement, financial services, technology platforms, and social media—to collectively address and disrupt the evolving tactics of scammers.

Table of Contents

1.0

Block’s purpose and addressing emerging risks

1.1

Block, risk management, and the digital age of financial services

Economic empowerment means that everyone should be able to participate and thrive in the economy.

In 2009, Square started by enabling anyone with a mobile device to accept card payments, anywhere, anytime. For one flat, clear rate, anyone could accept a credit card payment. The ease, speed, and transparency of the process was revolutionary. Millions of sellers who had previously been unable to accept card payments could now participate in a rapidly changing economy.

Square’s work to provide millions of small businesses with access to card payments for the first time required a differentiated approach to risk management. Square built technology to quickly detect and eliminate risky and fraudulent activity, allowing the company to approve sellers who may have been denied elsewhere, while keeping risk and fraud losses low.

As Square grew, it built increasingly complex and complementary systems — a mix of technology and human review — to manage risk across new products. For example, Square Loans is a service that offers loans to small businesses that use Square’s point-of-sale system. The scale of Square’s network enables a deep understanding of a business’s transaction volume and cash flow, which the company uses to proactively evaluate sellers and underwrite and extend right-sized loans to them. This has allowed Square to effectively manage risk — Square Loans’ loss rate is less than 3% — and has given millions of small businesses access to capital that they might otherwise have been unable to secure.[1]

Cash App was the company’s first foray into helping individuals, consistent with how Square made access to business tools easier for sellers. Since Cash App started in 2013, initially built to take the pain out of peer-to-peer (“P2P”) payments, the technology landscape has changed dramatically. Today, people have access to more technology, tools, and services than ever before, and they engage with financial services across multiple platforms, including social media and messenger apps. Of course, with each wave of innovation comes a new set of challenges, including the increasing complexity and sophistication of scams.

> For individuals in the U.S. especially, 2024 has been termed the “Golden Age of Scams,” with scams affecting a broad spectrum of the population both on and off the internet.[2,3]

As a member of the financial system, Block takes its responsibilities seriously and is dedicated to maintaining customer trust and safety by proactively addressing emerging risks and threats as the financial ecosystem continues to evolve.

In this constantly evolving environment, staying ahead of these challenges is a critical priority.

1.2

Scammers are creating major problems for consumers

Scams lack a precise definition but are generally considered a subset of fraud. Scams often involve tricking individuals into authorizing payments under false pretenses, whereas other types of fraud typically involve unauthorized transactions where consent is bypassed entirely.[4,5]

Recent data highlights the growing impact of scams, now among the four most common crimes affecting American households.

In the past 12 months,

15%

of U.S. adults reported that someone in their household had fallen victim to a scam.[6]

According to the Federal Trade Commission (“FTC”),losses from investment scams reached

$4.6B

and losses from impostor scams reached

$2.7B

in 2023.[7]

Consequently, consumer anxiety is rising — 57% of Americans rank scams involving financial access or payments as their second-greatest crime concern.[8]

FTC data further reveals that “Payment Apps or Services” are the third most common payment method cited in fraud reports, following credit and debit cards.[9] As a leader in P2P payments, Cash App provides tools and processes to help combat scams and educate consumers to safely enable payments.

2.0

The growing complexity of scams

One of the biggest challenges in defining scams is understanding their variety. There is no universal framework for categorizing different types of scams or for addressing them across all platforms. Scams also follow a distinct life cycle, often originating on communications platforms, such as social media or messenger apps, before moving in their final stage to soliciting a payment. The rise in digital activity with telephones, emails, internet, communication platforms, and especially social media has fueled the spread of scams as scammers become increasingly adept at identifying, engaging, and exploiting their victims with sophisticated tactics.

2.1

The challenge of categorizing scams

> “Scammers are constantly finding new ways to steal your money, from blackmail to romance scams to selling nonexistent items.”[10]

Scammers constantly evolve and change tactics, making it difficult to develop a universally accepted classification system for scams. This creates challenges in measuring their full scope within the financial services industry and distinguishing them from other types of fraudulent activity.

In response, several government agencies have formed working groups or issued guidance to outline common scam types. In 2023, the Federal Reserve Board (“FRB”) sought to establish an industry-standard definition of scams, agreeing on “the use of deception or manipulation intended to achieve financial gain.”[11] This definition emerged from a cross-industry working group of financial institutions focused on standardizing definitions and improving classification and prevention efforts. In June 2024, the FRB introduced its initial ScamClassifier model.[12,13] While these initiatives represent a significant step forward, they don’t fully address the classification challenges faced by the broader industry as these efforts largely concentrate on traditional financial institutions and overlook key players in the broader ecosystem, such as social media platforms and P2P payment services. Without broader inclusion of non-traditional platforms in these discussions, the industry’s ability to fully combat the evolving scam landscape remains limited, leaving gaps in protection for millions of consumers who engage with these digital services daily.

Recognizing the widespread threat of scammers in the industry, Cash App invests in understanding the unique needs and concerns of customers when it comes to scams, and designs solutions specifically aimed at keeping customers, and their money, safe. To design solutions specifically aimed at keeping customers, and their money, safe, Cash App has developed its own approach to better identify individuals’ experiences with the most prevalent P2P scams.. Leveraging knowledge from various industries and adopting a customer-first perspective, Cash App’s Behavioral Insights Team has analyzed a vast dataset of transactions to uncover patterns and typologies of scams. Through this research, the team created a taxonomy of distinct P2P scam types, categorized under two widely recognized groups: Impostor Scams and Deception Scams. The chart below outlines the type of scams that can be found across the industry across these two groups.

Impostor scams

Impostor scams involve the scammer pretending to be a known brand/business, government entity, family member, etc.

Brand/Business Impersonation

Scammers reach out to victims through channels such as email, text message, and phone call. The scammer's outreach outlines that there is an issue with one of the customer's existing or past accounts (e.g., Apple, Amazon, their local utility, healthcare provider) and that a payment must be made to resolve the situation. Other forms will involve scammers pretending to be the support team of reputable companies through social media posts, discussion boards, or fake websites. Rather than directly reaching out to potential victims, scammers will take advantage of individuals by pretending they are legitimate support individuals searching for remedies of an individual's existing issues (e.g., lost account access, trouble getting refunds).

Government Impersonation

Scammers reach out to victims pretending to be a government agency (e.g., IRS, Social Security Administration, FBI). In addition to phone calls, emails, and text messages, scammers may also send physical mail that mirrors the format and style of agency communications. In these cases, potential victims are directed to contact fake phone numbers or emails where scammers await to further convince potential victims. These scams are commonly centered around obligations owed, particularly taxes.

Friend/Family Impersonation

These scams are centered around an associate — known by the potential victim, and who is in need — typically involving a sense of urgency. This could range from requiring funds to pay back a debt or to post bail. These scams are made more convincing when the scammer can layer in details about the associate such as the relationship to the victim or a specific location.

Deception scams

Deception scams involve misleading victims into sending funds for a variety of purposes

Money "Flip" Scams

Scammers will claim they can "flip" a customer's money and multiply it as long as the customer first sends a payment. In some instances the scammer may send back the initial smaller flip in hopes of receiving an even larger amount later (e.g., returning $25 from a $5 flip to get $100 from the victim in the next iteration). These scams are prevalent on social media and can involve people falsely commenting that the scheme worked for them in order to induce others.

Goods and Services Scam

These scams involve goods or services that are listed or advertised at prices below normal market rates, and are prevalent on internet marketplaces, relying on convincing pictures and profiles to add a sense of legitimacy. Victims are often directed to pay upfront or provide a deposit, while the scammer does not possess or has no intention to provide the goods or services in question.

Romance Scam

Scammers adopt fake identities and enter into an online romantic relationship to gain a victim's affection and trust, often on dating apps and social media sites. Eventually, the scammer uses this relationship to manipulate and steal from the victim, often under the pretenses of facilitating travel or to address some financial hardship. Unlike other scams, these can develop over a significant period of time, such as weeks or months.

Job Scam

These scams take advantage of job seekers through fake job listings on job boards, social media, and classified sites. Scammers will ask for money under the pretense of placement, equipment, background check, or training fees.

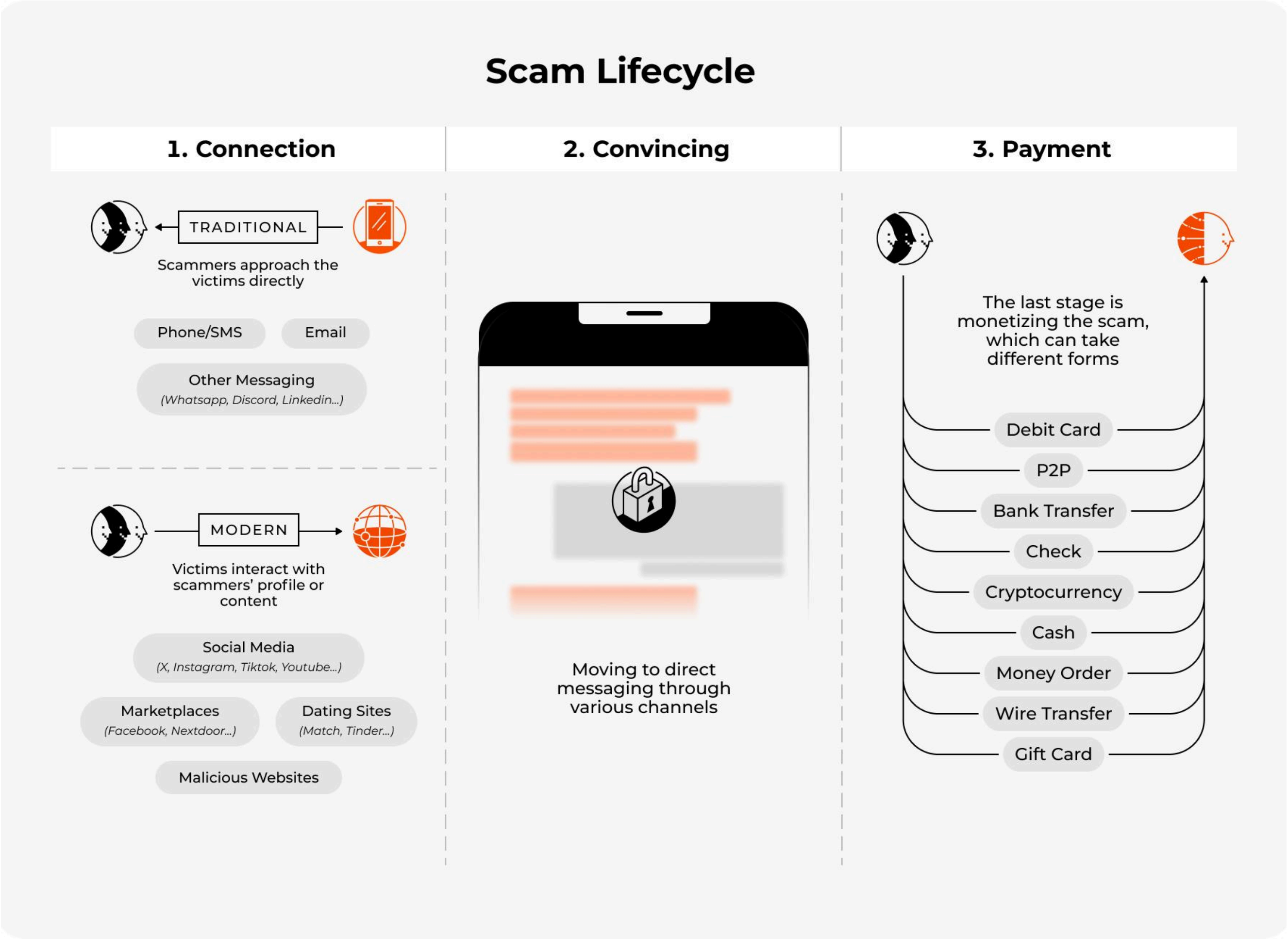
Investment Scam

Scammers convince victims to send funds purportedly to be invested on their behalf (e.g., stocks, crypto), often framed as "can't-miss" opportunities. These scams can increase in monetary value over time with initial "investments" showing strong returns in hopes of securing additional larger contributions from victims. These scams are often found on social media, online forums, and messaging apps.

2.2

Scams have an extensive lifecycle, involving multiple tools and platforms

Within the industry, it is widely recognized that scams often originate on other platforms and target individuals, with payment typically representing the final step in the scam lifecycle. Cash App has identified three distinct stages in this process: Connection, Convincing, and Payment.


Scam Lifecycle
1. Connection
2. Convincing
3. Payment
TRADITIONAL
Scammers approach the victims directly
Phone/SMS
Email
Other Messaging
(Whatsapp, Discord, Linkedin...)
MODERN
Victims interact with scammers' profile or content
Social Media
(X, Instagram, Tiktok, Youtube...)
Marketplaces
(Facebook, Nextdoor...)
Dating Sites
(Match, Tinder...)
Malicious Websites
Moving to direct messaging through various channels
The last stage is monetizing the scam, which can take different forms
Debit Card
P2P
Bank Transfer
Check
Cryptocurrency
Cash
Money Order
Wire Transfer
Gift Card

Connection

Scams begin with the scammer attempting to establish a connection with potential victims. Third-party research suggests there are various places where scam victims can be contacted — with social media, websites, and email being some of the most frequent.[14] The growth of internet platforms has enabled scammers to reverse their approach: rather than seeking out victims directly, they now create enticing posts or profiles on social media, online marketplaces, dating sites, or malicious websites, prompting victims to initiate contact themselves. For example, victims might discover an artist they like on Instagram's "For You" Explore tab and direct message the artist to commission particular work. Rather than delivering the work, the scammer may continue to request more money to complete a project that they never had the intention of getting done. Another example: In the comments section of a charity's YouTube video, a scammer posing as the charity's representative replies to a scam victim who is asking how to donate. Only one or two letters are changed in the profile name, which the scam victim easily overlooks.

FTC data shows that more money was reported lost from fraud (using their broader definition that includes scams) originating on social media than any other contact method. Out of nearly $9 billion of total losses reported from fraud between January 2021 and June 2023, approximately 30% originated on social media.[15]

Convincing

The second stage of a scam involves the scammer working to convince the victim of the scam's legitimacy. After initial contact, scammers often shift the conversation to a direct message through social media or messaging apps, where it may be harder for communications platforms and tools to detect the activity. There is evidence that this can be an effective tactic — scams that were initiated via text messages or messaging apps had some of the highest median dollar losses reported in 2023.[16]

Scammers use a range of manipulative tactics to achieve their goals. Some scams escalate quickly, creating a sense of urgency to pressure victims into making rushed decisions, while others, like investment and romance scams, unfold gradually to build a convincing narrative.[17,18,19] Regardless of the approach, the ultimate goal remains the same: to persuade the victim to part with their money or personal information, advancing the scam to its final stage.

Scammers deliberately move across platforms during a scam, making it harder for each individual platform to detect and prevent the activity. This behavior reflects a complex journey, with typical scams unfolding across multiple stages and involving several platforms along the way.

Payment

The final stage of a scam involves the actual payment of funds from the victim to the scammer. This typically occurs through one or more transactions using various methods such as prepaid cards, gift cards, credit cards, debit cards, check, cash, money orders, wire transfers, and P2P payment apps. As a result, financial institutions and payment platforms are positioned at the end of the scam life cycle, often with little to no visibility into the prior interactions between the scammer and victim. Increased information sharing among the entities would help to assess transactions at all stages of the scam lifecycle.

2.3

The rise in scams coincides with increased digital usage, especially social media

Research from the first quarter of 2023 shows that as people spend more time online — over 2 hours per day for the average American internet user, and even more for younger adults (Gen Z ≥ 4 hours per day) — their potential exposure to scams and fraud increases.[20,21,22]

Nearly

40%

of 2021 fraud loss reports by Gen Z and younger Millennials originated on social media, compared to older adults, who are more often targeted through phone calls.[23]

As consumer activity increasingly takes place online, people leave behind significant amounts of personal information. The challenge of the online environment is that a victim's own digital footprint can provide scammers with ample data to create convincing fake personas and tailor their approaches. A 2023 study by YouGov and the Trade Desk found that 74% of U.S. adults were willing to share personal details with brands and retailers when asked.[24]

This growing pool of data creates more opportunities for scammers, who use highly personalized outreach to make it harder for recipients to distinguish truth from deception. For example, in a Government Impersonation scam, victims may receive a message from someone falsely claiming to represent a government agency, such as the IRS, leveraging personal information to demand payment for an urgent, fabricated issue such as overdue taxes.

The increasing use of social media platforms for things beyond building connections, such as buying, selling, and promoting products and services, has enabled scams to proliferate.[25] These activities provide additional attack vectors for scammers to exploit. Goods and Services and Investment scams (referenced above) are two common examples that thrive on social media.[26,27]

Related, scammers have always sought to exploit payments — from wire transfers to money orders to checks — and their attempts to exploit new technologies such as digital payments are no different. Digital payment tools, such as Paypal, Venmo, Zelle, and Cash App, have exploded in popularity over the past decade and become an integral part of commerce — across P2P payments, e-commerce, and even small businesses.[28] The convenience, ease, and speed of these apps have made transactions much simpler and well-suited for younger individuals who are more technologically savvy.

Even though the digitally native generation, particularly Gen-Z, has grown up with social media and other online marketplaces, as well as digital payment tools, the blending of these worlds also makes it difficult to discern legitimate requests from scams — especially as scammers become more and more sophisticated in their tactics with fake social profiles, phishing messages, or fraudulent ads.[29]

2.4

Scammers are becoming increasingly sophisticated, blending technological, psychological, and operational strategies to exploit victims

The rise of artificial intelligence ("AI") has led to the development of tools that can generate convincing deep fakes, enabling scammers to impersonate trusted figures or fabricate realistic video and audio content. Even for simpler scams, generative AI chatbots are being utilized to enhance the text of phishing emails, making them less detectable.[30] New research suggests the full email phishing process — from collecting targets to optimizing email performance — can be effectively automated using large language models (LLMs), and industry experts expect the threat from AI-based scams to increase as the technology advances.[31,32]

AI also empowers scammers to analyze and exploit vast datasets of leaked or stolen personal information, which helps them target victims more effectively at scale and increases the credibility of their scams. The FRB has published research on the growing trend of creating synthetic identities, defined as identities generated by combining real information (such as a legitimate Social Security number) with fictitious details (like a false name, address, or date of birth).[33,34] While this practice is more closely related to other types of fraud — where these fabricated identities are used to max out credit lines with no intention of repayment — it underscores the escalating sophistication of both scammers and the tools at their disposal.

Scammers are also skilled at employing psychological tactics to manipulate victims. Research indicates that heightened emotional states can make individuals more susceptible to persuasion and fraud.[35,36] This can involve evoking emotions such as fear (for example, posing as a tax official), greed (such as promoting investment scams), or urgency (claiming that a bank account is at risk of immediate closure).[37]

Operationally, scammers are adept at tracking individuals across multiple channels, adapting to security measures, and quickly exploiting new vulnerabilities. This rapid adaptability poses a significant challenge for those working to combat these threats.

3.0

Cash App's approach to combating scammers

Given the increasing complexity of scams and the evolving tactics of malicious actors, Cash App adopts a multifaceted strategy that combines various approaches to effectively combat scams and safeguard its customers.

"2-Factor Authentication"
November 2024 (YouTube)

3.1

Customer awareness and education

Cash App continually seeks to protect, educate, and empower all of its current customers and the broader public to identify and take action against potential scams. Scams are a problem that affect everyone regardless of payment platform or method, so Cash App leverages a combination of targeted education and national, broadly distributed campaigns to reach consumers where they are.

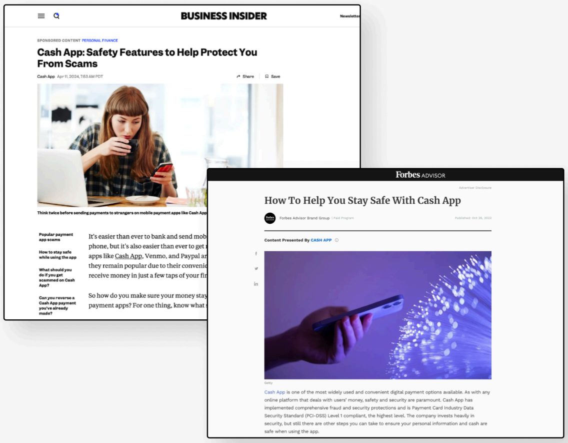
1. National campaigns across television, streaming video, social media, and radio
2. Partnering with third-party organizations
3. Cash App's website and support pages
4. Email marketing campaigns
5. Proactive social media presence

Cash App has run national campaigns to build awareness of scams, with one in December 2023 called "If it's weird for real, it's weird for real," which included multiple broadcasts during the NBA finals and NHL finals. This multi-channel brand campaign featured a series of videos aimed at educating individuals on how to be aware of common scam types including Money Flips, Business Impersonations, and Prize Scams. These videos were complemented with paid marketing efforts across multiple social media channels, meeting customers where they are (and where scams are often first encountered), on platforms such as Instagram, TikTok, X, and YouTube. This campaign delivered 53 million impressions.[38,39]

In addition, during the 2023 holiday season (a particularly vulnerable time for those in financial need), Cash App commissioned a satellite media tour with Cash App's Head of Security, who spoke with several local TV and radio stations across the country on how customers can protect themselves from fraud and scams.

The interviews ran and/or were syndicated more than 400 times across various channels (TV, radio, and online), reaching a total of 8.9 million media impressions.[40]

Cash App also developed partnerships with third-party publishers to raise awareness of scams and educate customers on how to protect themselves; this content has been seen across publications such as Forbes, AP News, Mashable, Refinery 29, and Business Insider. Working with publishers resulted in more than 2 million social views and drove individuals to Cash App's website and support articles about scams.[41]



SPONSORED CONTENT PERSONAL FINANCE

Cash App: Safety Features to Help Protect You From Scams

Cash App Apr 11, 2024, 7:53 AM PDT

Think twice before sending payments to strangers on mobile payment apps like Cash App

Popular payment app scams

How to stay safe while using the app

What should you do if you get scammed on Cash App?

Can you reverse a Cash App payment you've already made?

It's easier than ever to bank and send mob
phone, but it's also easier than ever to get
apps like Cash App, Venmo, and Paypal ar
they remain popular due to their convenie
receive money in just a few taps of your fi

So how do you make sure your money stay
payment apps? For one thing, know what

How To Help You Stay Safe With Cash App

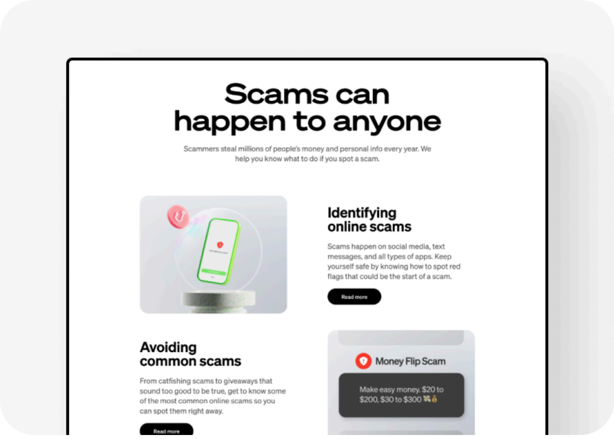
Forbes Advisor Brand Group | Paid Program Published: Oct 26, 2023

Content Presented By CASH APP

Getty

Cash App is one of the most widely used and convenient digital payment options available. As with any online platform that deals with users' money, safety and security are paramount. Cash App has implemented comprehensive fraud and security protections and is Payment Card Industry Data Security Standard (PCI-DSS) Level 1 compliant, the highest level. The company invests heavily in security, but still there are other steps you can take to ensure your personal information and cash are safe when using the app.

Cash App's website and support pages contain educational content such as Outsmart Scams, How to identify a scam and stay safe online, and 9 common scams and how to avoid them, providing customers and prospective customers with the tools to protect themselves.[42] Cash App also uses targeted email marketing campaigns to build just-in-time awareness of the tooling that aids Cash App's detection, warning, and blocking efforts (see 4.3 for more details).



Scams can happen to anyone

Scammers steal millions of people's money and personal info every year. We help you know what to do if you spot a scam.

Identifying online scams

Scams happen on social media, text messages, and all types of apps. Keep yourself safe by knowing how to spot red flags that could be the start of a scam.

Avoiding common scams

From catfishing scams to giveaways that sound too good to be true, get to know some of the most common online scams so you can spot them right away.

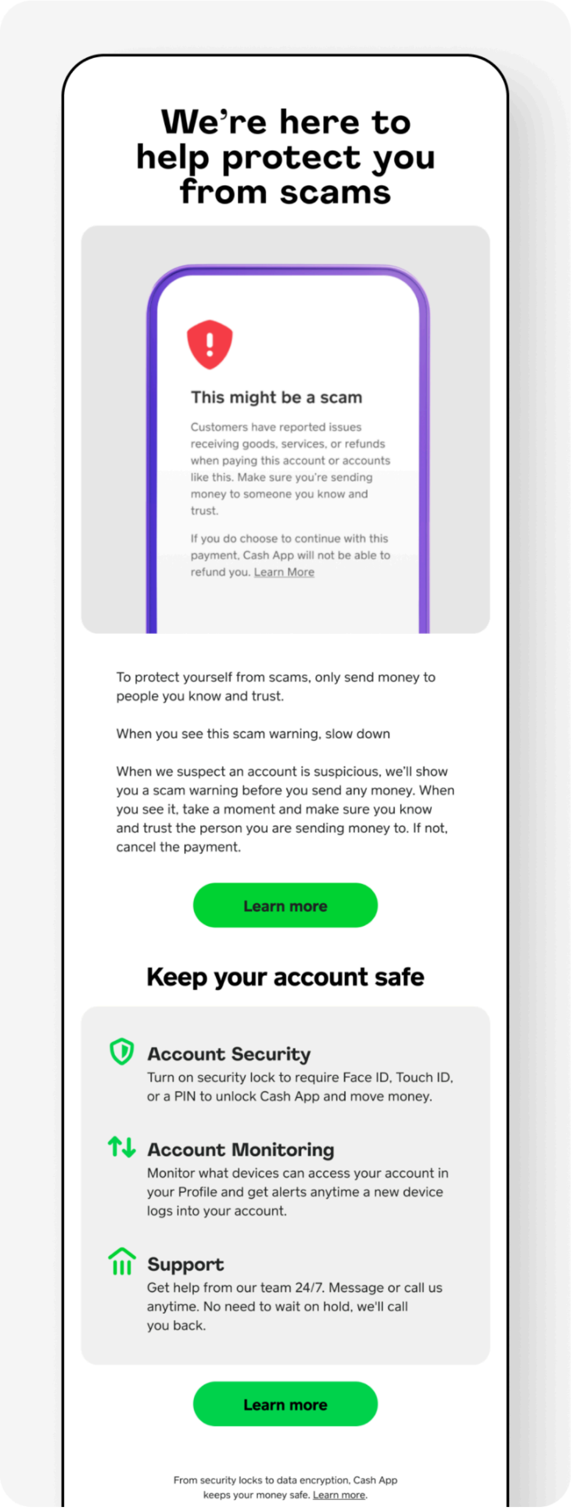
Money Flip Scam

Make easy money. $20 to $200, $30 to $300 💸💰

"Outsmart Scams" page on cash.app

Cash App also partners with third-party organizations to amplify safety messaging. In November 2023 and again in November 2024, Cash App partnered with the Financial Technology Association ("FTA") to launch a national scams-education campaign called Smarter than Scams, which focused on safe P2P practices, digital financial literacy, and consumer protection targeting key consumer markets across the U.S. In the most recent campaign, Cash App and FTA expanded its reach to include out-of-home advertising and a satellite media tour, which reached over 94 million customers across the U.S.[43]

In November 2024, Cash App launched the second iteration of the "If it's weird for real, it's weird for real" marketing campaign to demonstrate how Cash App actively keeps customers' money safe. The multi-channel campaign features videos highlighting Cash App's proactive account alerts and security features, including scam warnings, transaction alerts, one-time passcodes, and Cash App Card lock. These videos will be seen on streaming video platforms, social media channels, and live television, including during NFL games.



We're here to help protect you from scams

This might be a scam

Customers have reported issues receiving goods, services, or refunds when paying this account or accounts like this. Make sure you're sending money to someone you know and trust.

If you do choose to continue with this payment, Cash App will not be able to refund you. Learn More

To protect yourself from scams, only send money to people you know and trust.

When you see this scam warning, slow down

When we suspect an account is suspicious, we'll show you a scam warning before you send any money. When you see it, take a moment and make sure you know and trust the person you are sending money to. If not, cancel the payment.

Keep your account safe

Account Security
Turn on security lock to require Face ID, Touch ID, or a PIN to unlock Cash App and move money.

Account Monitoring
Monitor what devices can access your account in your Profile and get alerts anytime a new device logs into your account.

Support
Get help from our team 24/7. Message or call us anytime. No need to wait on hold, we'll call you back.

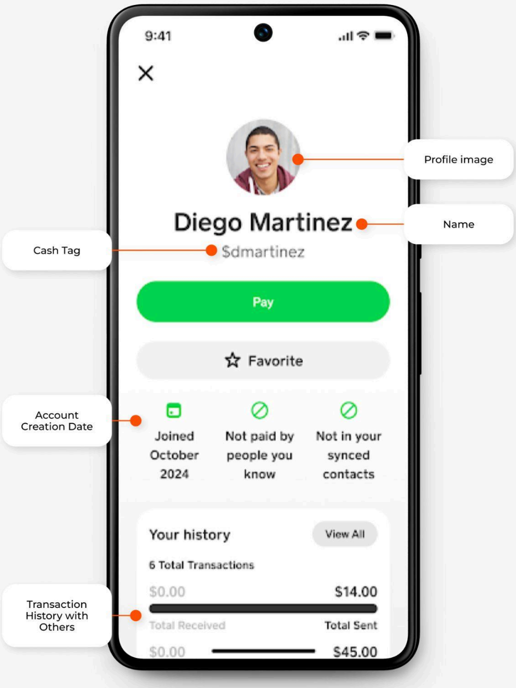
From security locks to data encryption, Cash App keeps your money safe. Learn more.

"We're here to help protect you from scams" email campaign

3.2

Customer profiles

When using Cash App, customers can review the profiles of other accounts before initiating payments. These profiles feature various elements designed to help customers understand the identity and trustworthiness of the recipient. These include the account creation date, transaction history with others in the customer's network, whether the recipient is in the customer's synced contacts book, profile image, name, and $cashtag. By providing this information, Cash App helps customers make more informed decisions before transferring funds.



9:41

Diego Martinez

$dmartinez

Joined October 2024

Not paid by people you know

Not in your synced contacts

Your history

6 Total Transactions

Total Received	Total Sent
$0.00	$14.00
$0.00	$45.00

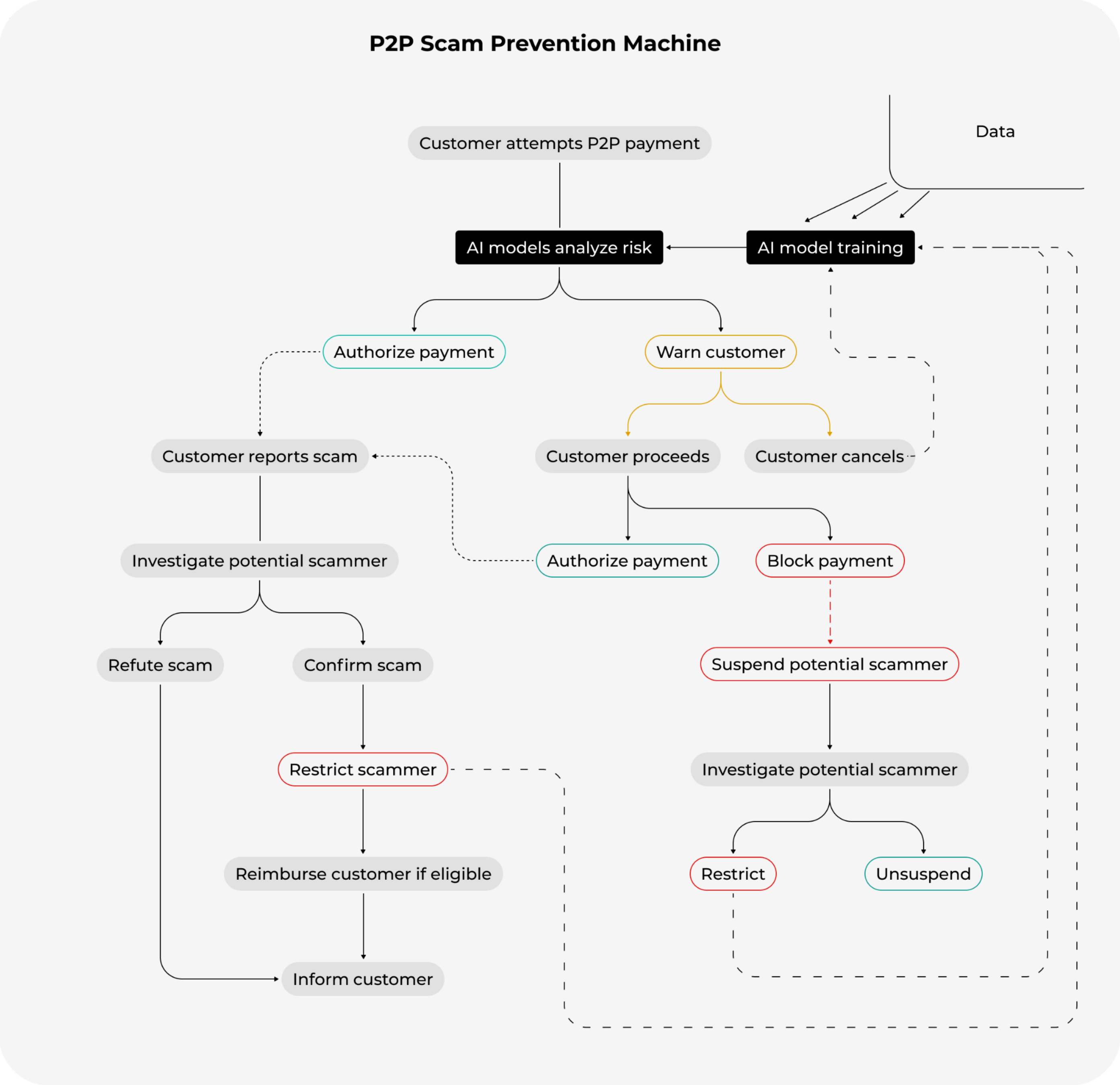
Cash App profiles designed to help customers understand the identity and trustworthiness of recipients

3.3

Cash App’s P2P scam prevention machine

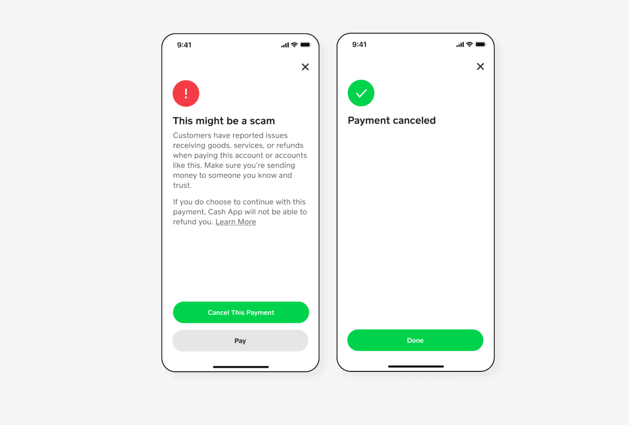
Cash App leverages advanced internal mechanisms to combat scam activity and minimize customer risk. This strategy is driven by AI models that continuously assess payment attempts and customer behaviors, allowing for timely interventions such as warnings, blocks, and escalations for further reviews.

These AI models utilize extensive data from the Cash App ecosystem, including customer attributes, transaction history, and customer reporting. Recognizing that customer reporting provides invaluable insights, Cash App prioritizes making the reporting process straightforward and gathers essential information to support investigations and enhance future detection capabilities. Additionally, Cash App benefits from a dedicated fraud investigation team that thoroughly examines specific accounts flagged by either customer reports or AI models.



3.3.1
Detection and warning

A key aspect of our approach for Cash App is to detect and warn customers about potential scams before their transactions. To achieve this, Cash App uses advanced AI models specifically designed to detect P2P payment scams in real-time across millions of attempted transactions daily.[44] These models are trained on extensive historical data sets from Cash App activity, including customer data, transaction histories, and customer reports. The models are continually refined and updated to ensure they utilize the most current data available.



This might be a scam

Customers have reported issues receiving goods, services, or refunds when paying this account or accounts like this. Make sure you're sending money to someone you know and trust.

If you do choose to continue with this payment, Cash App will not be able to refund you. Learn More

Payment canceled

Scam Warning and Cancellation

When the AI models identify a high-risk payment, Cash App activates its Payment Warnings tool, which displays an in-app pop-up alerting customers that their transaction may be linked to a scam — as of the end of November 2024, scam warnings were deployed on approximately 1.2% of peer-to-peer payments per week on average.[45] Given that many scams rely on instilling a sense of urgency, these warnings serve to slow down the transaction process, allowing customers the opportunity to look at the trust signals, reconsider their payment, and, if necessary, cancel it. While the warnings can encourage customers to reassess before proceeding, they do not mean that a scammer is involved every time. When customers receive a scam warning, they abandon or cancel their payment 37% of the time, avoiding more than half of funds associated with those warnings, demonstrating the effectiveness of the tool.[46]

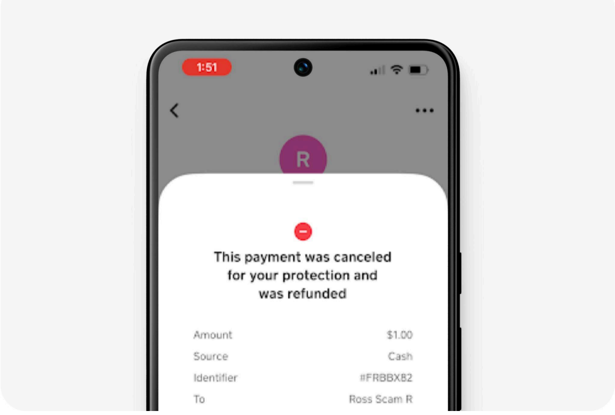
One Cash App customer noted:

"I saw a pop up from Cash App that said this person has been reported a lot as a scammer - when this pop up came up and I saw this I didn't send the money and reported him and blocked him."

3.3.2
Blocking and suspending

If a customer chooses to proceed with a flagged payment despite receiving a warning, Cash App's AI models will assess the transaction for risk and, depending on the transaction, Cash App may automatically block it and return funds to the sender. The customer will receive a notification explaining that the payment will not be completed.

In many cases, following this automatic payment blocking, Cash App will also suspend the suspected scammer's account, temporarily preventing the account from being able to receive payments until further investigation occurs confirming a scam occurred. In these instances, Cash App will also issue a scam warning to the potential victim for all of their payments for a short period of time in case the scammer attempts to redirect them to another account. This allows Cash App to block high-risk payments and suspend high-risk accounts in real time.



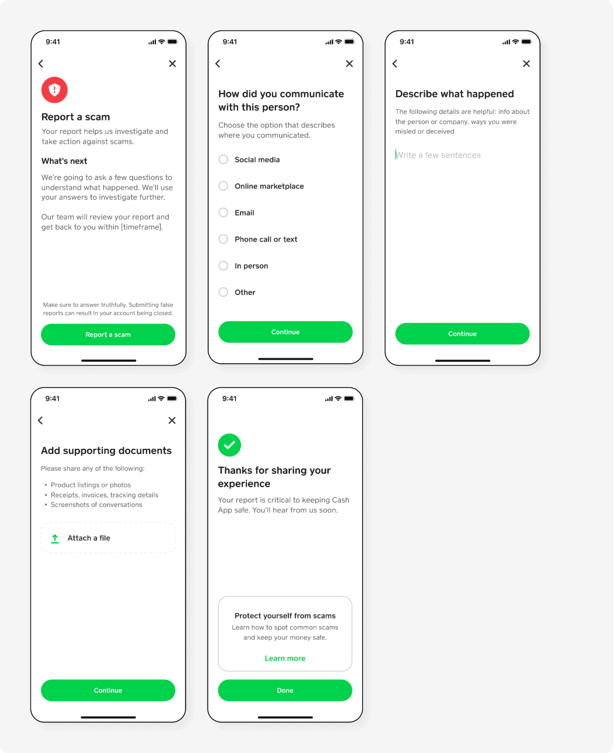
This payment was canceled for your protection and was refunded

Amount	$1.00
Source	Cash
Identifier	#FRBBX82
To	Ross Scam R

3.3.3

Customer reporting & remediation

When scams do occur, Cash App simplifies the reporting process for customers through an in-app feature known as “Scam Reports,” allowing customers to protect themselves and others on the platform. By reporting scams, customers help Cash App prevent further victimization by the same scammers and can stay ahead of emerging threats. These reports play a crucial role in updating AI models designed to warn customers and block potentially fraudulent transactions related to scams. Additionally, this reporting system helps in educating customers about emerging scam trends, taking action on confirmed scammers, and reimbursing qualifying confirmed scams.



Report a scam

Your report helps us investigate and take action against scams.

What’s next

We’re going to ask a few questions to understand what happened. We’ll use your answers to investigate further.

Our team will review your report and get back to you within [timeframe].

Make sure to answer truthfully. Submitting false reports can result in your account being closed.

How did you communicate with this person?

Choose the option that describes where you communicated.

○ Social media
○ Online marketplace
○ Email
○ Phone call or text
○ In person
○ Other

Describe what happened

The following details are helpful: info about the person or company, ways you were misled or deceived

Write a few sentences

Add supporting documents

Please share any of the following:

- Product listings or photos
- Receipts, invoices, tracking details
- Screenshots of conversations

Thanks for sharing your experience

Your report is critical to keeping Cash App safe. You’ll hear from us soon.

Protect yourself from scams

Learn how to spot common scams and keep your money safe.

Cash App Scam Reporting feature (abridged)[48]

Cash App has started to roll out an enhanced scam reporting process, which is expected to be fully available to all customers in early 2025. This new reporting flow includes structured data collection regarding the method of the scam (e.g., social media, email, text message, etc.), the nature of the scam (e.g., impostor, deception), and the type of scheme (e.g., goods/services scam, financial reward, etc.), alongside a freeform entry for customers to describe their experience and provide supporting documentation (e.g., screenshots). This additional information has multiple benefits including (1) improving the ability to confirm whether a scam has occurred, (2) enabling Cash App to remove scammers from the platform more quickly and accurately, (3) enhancing data granularity for ongoing detection improvements, and (4) improving educational resources about recent trends. Since implementing this updated reporting flow, Cash App has significantly increased its capability to confirm scams, and therefore remove bad actors from its platform.[47]

Reimbursement program

Over the past year, Cash App has developed a scam reimbursement policy — covering confirmed Impostor and Deception scams — where claims are reviewed by a fraud specialist, who determines whether an actual scam occurred. In mid-2024, Cash App began testing scam reimbursements for eligible Cash App customers. By definition, scams are transactions authorized by the customer, and thus ineligible for other dispute processes. A well-constructed reimbursement program, however, can reduce negative impact on customers, incentivize timely and accurate reporting, and serve as another opportunity for customer education.

Given the current industry-wide challenges with respect to first-party fraud and large-scale abuse of disputes programs, Cash App has included some limits within this policy to help prevent abuse of the program while allowing for broad coverage of confirmed scam incidents.

Under Cash App’s current scam reimbursement policy, customers may be eligible for partial or full reimbursement for confirmed Impostor and Deception scams reported within 60 days of the payment if they did not receive an in-app pop-up warning them of the risks of proceeding at the time of the payment.

As of the end of November, Cash App reimbursed more than 20,000 customers that fell victim to a confirmed scam, and nearly 90% of those customers were fully reimbursed. Similar to the new scam reporting flow described above, Cash App expects its scam reimbursement program to be fully rolled out in early 2025.[49]

Within Cash App's current policy limits, customers receiving reimbursement are fully reimbursed nearly

90%

of the time

3.3.4
Investigations and removing bad actors

Cash App also leverages its team of fraud specialists to perform timely reviews and investigations into scam claims and high-risk accounts (e.g., suspended accounts). Fraud specialists leverage advanced internal tooling that provides detailed customer information, transaction history, connections to other accounts, claim details, and more. These tools allow Cash App's agents to thoroughly review scam claims and high-risk accounts to confirm claims, which support the reimbursement process, and take any other necessary actions. When Cash App's specialists identify a scammer account, they restrict the account, any identified associated accounts, and unique assets associated with the scammer (such as SSNs and devices) to prevent them from returning to the platform in the future.

Cash App's prompt actions against potential scammers support customer safety and long-term trust.

Removing scammers from the platform in a timely manner is a core priority. This is also one of the primary benefits of Cash App's improved scam reporting flow: collecting more information from customers — such as originating platform, scam details, and screenshots — to help fraud specialists investigate and confirm claims in conjunction with other internal signals.

3.3.5
Work outside Cash App

Given that most scams originate outside its platform, Cash App invests resources to combat scams at their source — primarily social media and other online platforms. These efforts not only protect Cash App customers but also benefit individuals more broadly.

Cash App reduces online scam activity by partnering with third-party vendors that monitor social media platforms, domain names, and URLs for unauthorized use of Cash App brand assets alongside scam-related keywords, icons, and images. Following their analysis, these vendors issue takedown notices to the respective platforms for fraudulent social media accounts, websites, and domains, and ensure follow-up until the content is removed. From January through August 2024, this process resulted in the takedown of over 6,000 social media accounts, websites, and domains.[50] Continued collaboration with social media platforms has resulted in a 25% improvement in the average number of days to remove scam-related accounts, reducing the duration of potential consumer exposure to these scams.[51]

In early 2024 Cash App introduced the Social Media Guardian, a tool designed to monitor scam activity beyond its platform, including responses to Cash App posts and mentions on social media. This system retrieves and analyzes data in real time to suppress posts identified as scam-related by internal detection models, preventing fraudulent accounts from tagging or responding to Cash App in the future. As of October 2024, this capability is live for both X and Instagram. Using this approach, Cash App has been able to identify and suppress with a high degree of accuracy thousands of scam-related posts weekly across these platforms.[52]

3.4 Measurement

Cash App has been successful in its initiatives to reduce the amount of scams on its platform as the Confirmed Scam Rate has been less than 0.01% of all peer-to-peer payment transactions on the platform as the new scam reporting flow continued to roll out.[53]

the Confirmed Scam Rate has been

<0.01%

of all peer-to-peer payments on the platform

To measure this, Cash App leverages data from the scam reporting flow to understand scams as a percentage of total payment transactions. Cash App strives to improve this percentage, and believes the efforts described above will continue to help over time. **In recent months Cash App has seen a significant decrease in the Confirmed Scam Rate as a direct result of efforts mentioned in this paper.**[54]

4.0

Building a united front against scams

As digital scams grow more complex and sophisticated, no single company can combat this threat alone. Cash App's commitment to protecting individuals is clear, but addressing the full scale of this problem demands collaboration across sectors. The path forward requires strong partnerships between government, law enforcement, financial services, telecommunications, social media, and technology platforms. Many scams begin well outside the financial services ecosystem, with scammers taking advantage of social media, marketplaces, and other online platforms to target potential victims. A united, multi-stakeholder approach across all industries is crucial for meaningful progress.

Cash App has invested heavily in this collective work — partnering with others across industries and the public sector to develop best practices, improve information sharing, and disrupt scams before they impact individuals. Through efforts like hosting regular in-person summits with law enforcement, Cash App is building the connections and fostering the transparency necessary to create a safer environment for customers. Block also recently joined the National Task Force on Fraud and Scams, launched by the Aspen Institute, and aimed at solving for a cross-industry coordinated national response to these crimes. These partnerships allow Cash App and others to gain a clearer view of criminal behaviors across platforms and to design proactive, resilient defenses that prevent scams at their origin. Cash App's approach to developing secure, scalable solutions aims to protect its customers and to contribute to the security of the larger digital ecosystem.

A call to action for industry-wide collaboration

1. *Educate and empower individuals:* Tackling scams goes beyond platform-specific measures — raising awareness among individuals is key to reducing vulnerability across their digital lives. While deeply committed to consumer education as mentioned above, Cash App is committed to joining with partners in an industry-wide effort to deliver timely, effective education that empowers individuals to recognize and avoid scams. Meeting individuals where they are to raise this awareness is a critical step in the fight against scams.

2. *Formalize information sharing:* It is time to establish a formal, cross-industry coalition dedicated to sharing threat intelligence and best practices in real time. This partnership would include financial services, law enforcement, social media, ISPs, and other key players, sharing information on what types of scams each is encountering and helping to coordinate effective responses and accelerate the development of technology-led solutions to detect and prevent scams.

3. *Strengthen resources for law enforcement:* For law enforcement to effectively combat scams, they need sufficient resources to investigate complex cases, prosecute high-level crime rings, and address lower-dollar frauds that disproportionately affect individuals. Providing these agencies with funding and tools can enhance law enforcement's capacity to investigate and curb this pervasive issue.

Cash App remains committed to standing alongside its partners in this fight against scams. Together, through transparent collaboration, education, and resource-sharing, there can be a safer digital world, empowering and protecting individuals with resilience and trust across platforms.

References and Notes

[1] Represents data as of Q3 2024

[2] Alana Semuels, "Welcome to the Golden Age of Scams," TIME Magazine (September 18, 2024)

[3] Lydia Saad, "Scams: Relatively Common and Anxiety-Inducing for Americans," Gallup (November 21, 2023)

[4] Association of Certified Fraud Examiners: Fraud 101: What is Fraud?

[5] PayPal, Fraud vs. Scams, Explained (October 12, 2023)

[6] Lydia Saad, "Scams: Relatively Common and Anxiety-Inducing for Americans," Gallup (November 21, 2023)

[7] Federal Trade Commission, "As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public, FTC," (February 9, 2024)

[8] Lydia Saad, "Scams: Relatively Common and Anxiety-Inducing for Americans," Gallup (November 21, 2023)

[9] Federal Trade Commission, Consumer Sentinel Network: Data Book 2023, page 11 (February 2023)

[10] CFPB "What are some common types of scams?", March 2024

[11] See Federal Reserve, 2023

[12] See Federal Communications Commission, Scam Glossary; Consumer Financial Protection Bureau, "What are some common types of scams?" (March 13, 2024); Federal Bureau of Investigation, Common Frauds and Scams.

[13] Federal Reserve Board Fed360, "Federal Reserve introduces the ScamClassifier Model," (June 17, 2024)

[14] BBB Institute for Market Trust, 2023 BBB Scam Tracker Risk Report (2023)

[15] Federal Trade Commission Consumer Protection Data Spotlight, Social media: a golden goose for scammers (October 2023)

[16] See BBB Institute for Market Trust, 2023 BBB Scam Tracker Risk Report, page 22, USD losses (2023).

[17] Elisabeth Carter, "Confirm Not Command: Examining Fraudsters' Use of Language to Compel Victim Compliance in Their Own Exploitation," The British Journal of Criminology, Volume 63, Issue 6, 1405–1422 (January 2023)

[18] Kendra Cherry, MSEd, "There's a Reason Even the Smartest People Fall for Scams," Verywell Mind (September 17, 2024)

[19] TD Bank, Advice on how to protect yourself from romance scams (February 20, 2024)

[20] See Viswanath, "Habitual Facebook use and its impact on getting deceived on social media," 2014

[21] Statista, Average daily time spent on social media according to global internet users as of the first quarter of 2023, by territory (2023)

[22] Ellyn Briggs, "Gen Z Is Extremely Online," Morning Consult (December 12, 2022)

[23] See FTC, Who experiences scams? A story for all ages December 2022

[24] See study results detailed in The Current, 2023

[25] McKinsey & Company, "Social commerce: The future of how consumers interact with brands," (October 19, 2022)

[26] Better Business Bureau, "BBB Scam Alert: Crafty scam targeting Facebook Marketplace sellers" (June 24, 2022)

[27] Amanda Hoover, "Scammers Are Ruining Facebook Marketplace," Wired (December 22, 2023)

[28] McKinsey & Company, "Fintechs, a new paradigm of growth" (October 24, 2023)

[29] Federal Reserve Bank of Kansas City, "Social Media for Personal Finances: A New Trend for Millennials and Gen Z" (October 11, 2023)

[30] Sam Sabin, "ChatGPT-written phishing emails are already scary good," Axios (October 24, 2023)

[31] Fredrik Heiding et al. "Devising and Detecting Phishing Emails Using Large Language Models," IEEE Access, Volume 12 (March 11, 2024)

[32] Fredrik Heiding, Bruce Schneier, and Arun Vishwanath, "AI Will Increase the Quantity — and Quality — of Phishing Scams," Harvard Business Review (May 30, 2024)

[33] McKinsey & Company, "Fighting Back Against Synthetic Data Fraud" (January 2, 2019)

[34] Federal Reserve, "Mitigating Synthetic Identity Fraud in the U.S. Payments System" (July 2020)

[35] See Norris and Brookes, "Personality, emotion and individual differences in response to online fraud", February 2021

[36] See the Federal Reserve Fed Payments Improvement: Scams, 2024

[37] See The Conversation, 2024

[38] Other examples of these efforts include: Cash App Wisdom: Account Protection (Twitter and Instagram); Cash App Wisdom: Cash Flipping Scam (Twitter and Instagram); Cash App Wisdom: Online Impostors (Twitter and Instagram); How to Avoid Common Scams (YouTube); Recognize Scams and Keep Your Money Safe with Cash App (Cash App Support); Don't Fall for Cash Flip Scams (YouTube and Instagram); Don't Fall for Customer Service Scams (YouTube and Instagram); Don't Fall for Giveaway Scams (YouTube and Instagram).

[39] Cash App internal data

[40] Cash App internal data gathered from Critical Mention, Nielsen Audio Daypart Cume data, various radio stations, and Similarweb.

[41] Cash App internal data, September 2024

[42] Other examples include: Recovering from a scam: What comes next?, Survey scams: What's real and what isn't?, Money flip scams: Everything you need to know, How to avoid scams on Facebook and social media, and How to spot a fake giveaway.

[43] Cash App internal data, November through December 2024

[44] Cash App internal data, January through September 2024

[45] Cash App internal data, November 2024. Scam warnings were deployed on approximately 1.2% of payments over a trailing 7-day period as of November 30, 2024.

[46] Cash App internal data, January through November 2024. As Cash App continues to expand warnings over time, this number would be subject to change.

[47] Cash App internal data, November 2024. Scam "confirmation" occurs when an agent is presented with a customer-submitted scam report and investigates the claim information and the behaviors of the reporter and reported account in accordance with documented procedures. Reports that Cash App determines to be actual scams are considered confirmed.

[48] Illustrative customer experience examples. These may change as Cash App continues to test features.

[49] Cash App internal data, January through November 2024. Cash App's policies are subject to change.

[50] Cash App internal data, January through August 2024

[51] Cash App internal data, January through August 2024

[52] Cash App internal data, October 2024

[53] Cash App internal data, Data represents from September 1 through November 30, 2024. Cash App's Confirmed Scam Rate is the percentage of confirmed scams relative to all peer-to-peer payment transactions within the new reporting flow treatment group in a certain period.

[54] Cash App internal data, November 2024

The charts and customer experience screenshots included in this paper are provided for illustrative purposes only. They may not accurately represent the exact customer experience within the App and are subject to change in the normal course of updates and improvements.