Peer-to-Peer Payment Apps

A Case Study for a Digital Finance Standard

JANUARY 24, 2023

Consumer Reports

Table of Contents

Executive Summary

The digital finance marketplace is rapidly changing and evolving, with new forms of payment, new forms of investing, new ways to borrow and spend, and new kinds of currencies. Consumers must navigate this dynamic financial ecosystem, with its constant flood of new products, but they don't have the information they need to make informed choices.

Between August and October 2022, Consumer Reports conducted an initial study examining the safety, privacy, and transparency of representative products in the peer-to-peer (P2P) payment systems industry: Apple Cash, Cash App, Venmo, and Zelle. We based this examination on a subset of the principles CR has established in its new Fair Digital Finance Framework. Specifically, the Safety Principle is used to evaluate the technology and policies that companies use to protect consumer data and funds; the Privacy Principle concerns company data collection, sharing, and deletion policies; and the Transparency Principle concerns company disclosures of legal terms and consumer legal rights.

Key Findings

- P2P payment apps collect large amounts of consumer data, often share data with other companies, and often make it difficult for consumers to delete the data.
- Policies for resolving fraud and errors can leave consumers at risk of losing money.
- App disclosures and documentation contain vague descriptions of security measures; there may be discrepancies between companies' disclosed security protocols and their practices.
- Users have to meet sometimes-confusing conditions to ensure that their funds are covered by insurance under the Federal Deposit Insurance Corp. (FDIC).
- Apps make it difficult for users to understand and track updates to legally binding documentation.
- Users are generally required upon sign-up to give up certain legal avenues for resolving potential disputes.
- Consumer disclosures are often difficult to find and read, reflecting a broad concern about transparency.

Introduction: The Case for a Fair Digital Financial Marketplace

Consumer Reports' vision for a Fair Digital Financial Marketplace is one in which digital financial products let consumers spend, save, borrow, and invest safely; respect their privacy and data; provide the benefits they expect; and protect them from discriminatory and predatory practices—all while helping them achieve their financial goals. We intend to promote that vision by providing timely, independent, and reliable reviews of the newest technology-driven digital finance products and services.

This is a critical moment for such an endeavor. The consumer finance marketplace has expanded exponentially over the past decade.[1] CR's August 2022 American Experiences Survey found that 83 percent of consumers use at least one type of mobile app to manage their financial needs and that consumers each use an average of two types of financial apps.

The mere availability of app-based and other digitized financial services, of course, does not mean that these products are safe, that they responsibly manage consumer information, or that they are meaningfully transparent. Indeed, in CR's survey 65 percent of Americans said they are somewhat or very concerned about how much information financial apps collect and store about their users. And over half believe that financial apps should not be allowed to share user data with other companies.[2]

The financial marketplace has also recently embraced certain aspects of inclusion,[3] and digital financial products in particular hold the promise of helping more consumers meet financial goals and achieve prosperity by integrating personal finance management into banking, payments, savings, investment, and money management apps, for little to no cost.[4] Whether fintech companies are sufficiently delivering on this promise, however, is an important question that the Fair Digital Finance Initiative will address.

This is not the first time Consumer Reports has set out to evaluate technology-driven digital finance products and services. In 2018, we applied the Digital Standard—a

[1] Toplin, J., "US Mobile Peer-to-Peer Payments Forecast 2022," *Insider Intelligence,* May 2022.
[2] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,123 U.S. adults, August 2022.
[3] Aspen Institute Financial Security Program, "Building an Inclusive Financial System: A Global Economic & Social Imperative for This Decade," July 2021.
[4] World Economic Forum, "Digital Tools Can Protect Consumers From Inflation, Here's How," August 2021.

framework for evaluating the privacy, security, ownership, and governance of consumer technologies—to peer-to-peer payment apps. That effort determined that:

1. It was very difficult for users to understand their rights and obligations in the event of error or fraud;
2. users could easily misdirect a payment to the wrong recipient;
3. fraud was a growing problem, and P2P services were not legally required to return or recover the funds; and
4. the apps collected a lot of user data but offered little information about how that data would be handled and used.

At the time of the 2018 tests, we estimated that 79 million Americans would use P2P payment apps that year. Today, the number is around 150 million,[5] and yet this recent evaluation—almost five years later—reveals similar opportunities to improve the consumer experience in 2022.

During those 2018 tests, we also recognized that the Digital Standard was not ideally suited for evaluating financial services products. Compared with the nonfinancial technology platforms and apps that the Digital Standard was developed to examine, financial laws and best practices set different—and typically higher—privacy, security, and governance standards for banks and financial institutions. To address these distinct needs, Consumer Reports had to develop a new framework and process for examining and testing digital finance products.

Over the coming year, in addition to peer-to-peer (P2P) payment systems, Consumer Reports will apply this framework and test other digital finance products and services such as buy now, pay later loans; banking apps offered by both traditional and online-only banks; and digital currency exchanges and wallets. Subsequently, Consumer Reports will expand its comparative evaluations into other product areas, such as apps for credit scores, savings and investment, and more.

[5] Toplin, 2022.

Methodology

The Fair Digital Finance Framework

CR's Fair Digital Finance Framework includes criteria, indicators, and procedures to test digital finance products across the principles of Privacy, Safety, Transparency, User-Centricity, Financial Well-Being, Inclusivity, and Environmental Social Governance. Each of these principles in the Framework contains multiple criteria that are then further broken out into indicators (actions or behavior demonstrating the criteria), and each indicator is assigned one or more testing procedures.

To develop the Framework, we completed a landscape analysis of domestic and international research-based and regulatory standards, frameworks, and guidelines. From this analysis, we chose the principles driving important digital finance policy considerations and consumer outcomes. Further, in addition to review by external stakeholders (industry representatives, academics, consumer advocates, and regulators), we engaged an external vendor to develop a parallel framework to: 1) validate the criteria in the Framework, 2) check for bias, 3) identify additional procedures and methods to test products, and 4) provide process development support for data collection and refresh techniques.

P2P Case Study Comparative Evaluations

The primary goal of this first case study evaluation is to test the Framework as a methodology and to engage the financial services ecosystem in order to iterate on the Framework.

This initial case study evaluation examined four peer-to-peer payment services: Apple Cash, Cash App, Venmo, and Zelle.[6] Though each offers its own blend of specific features, they all deliver the same core service: enabling individuals to digitally transfer money to, and receive money from, other individuals. This core feature was the focus of the initial testing. Other features, including crypto currency trading and more traditional credit offerings, as well as the privacy and security implications of such services, were

[6] For this first case study evaluation, we selected apps as representative of the peer-to-peer payments industry. The four apps were selected from those that offer P2P transfers as their primary service and were chosen based on their market share.

beyond the scope of this initial testing. (More information about each service can be found in Appendix 1.)

The evaluations, performed by Consumer Reports in August through October 2022, focused on operational and data policies of mobile versions of the peer-to-peer payment services. The analyses included a review of publicly available documents found on peer-to-peer company websites and mobile apps under headings such as “terms of service,” “terms and conditions,” “privacy policy,” “privacy disclosures,” and “end user license agreements” (sometimes shortened to “EULAs”). In this report, we will refer to these materials collectively as “documentation.”

These publicly available documents were evaluated in relation to the first three principles of the draft Fair Digital Finance Framework: Safety, Privacy, and Transparency.

- **Safety:** We examined disclosures of payment authentication controls available to users to prevent fraud and error, error resolution policies, whether providers ensure that funds they hold are covered by deposit insurance, and data security protocols such as encryption, authentication, security oversight, security over time, and vulnerability reporting.

- **Privacy:** We examined disclosures regarding data collection, minimum data collection, data usage, data sharing, minimum data sharing, data deletion, user data rights (rights to access, rights to correct), prioritization of privacy, and data retention.

- **Transparency:** We examined meaningful privacy disclosure, business model transparency, transparent safety practices, fair marketing, and meaningful explanation of service to determine whether consumers can protect themselves by easily reading documentation; whether users are required to agree to binding arbitration as a means of resolving potential disputes; and whether consumers can participate in class-action lawsuits in certain cases.

Because we examined only publicly available documents, no user accounts or personas were created to complete these comparative evaluations.[7]

In addition to customer service or help features in an app, clear and accessible documentation can often mean the difference between a consumer successfully

[7] Appendix 3 contains a more detailed account of this study’s methodology.

managing a challenging moment or being stuck and unable to satisfactorily resolve a problem. Thus, as an initial test of our Framework, we put ourselves in the place of consumers trying to evaluate not just what documentation is available but also how easy it is to locate various policies and disclosures, whether the language used is specific or vague, and whether the language is consistent across various policies.

Notably, we found a range of practices that are likely to challenge consumers in significant ways. Specifically:

- Different descriptions were used to describe the same processes, rights, and obligations across documentation sets, in app and online.
- In some instances, privacy policies and user agreements repeatedly link to other disclosures on the same issue without clearly indicating which policies govern for the purpose of data sharing and data collection. (For example, Apple's main privacy policy links to privacy policies for the App store, Apple Cash, and iTunes.)
- Outdated policies were still available to consumers, both online and in app.
- Documentation often contained contradictory information about notification and consumer rights. For example, across all companies we observed instances where companies specified how consumers would be notified about policy changes, followed by language that explicitly changed consumer terms and conditions or limited consumer rights to be notified about such changes.

We also met with the P2P companies before publication, giving them an opportunity to address concerns raised and give feedback on the Framework; the companies were then given an opportunity to answer specific follow-up questions on the record.

Spotlight on Transparency: Consumer Survey and Evaluation Insights

Consumer Reports conducts surveys on a regular basis to understand consumer concerns. We surveyed consumers on different aspects of their experiences and opinions about P2P payment services on four occasions in our monthly, nationally representative omnibus American Experiences Survey in 2022: in March, August, September, and October. These surveys add rich information about consumer experiences and enable us to evaluate subjective criteria in the Fair Digital Finance Framework.

For the purpose of this first case study on P2P payments services, it is worth noting that one topic highlighted by the survey and evaluation findings is transparency.

The survey findings suggest that consumers clearly need more, easy-to-understand information about whether their money is FDIC-insured, what types and amounts of personal data are being collected by the apps, and how that data are being used. In the October 2022 CR survey, consumers said they lack some basic information about these financial apps, as indicated by these findings:

- Only about half of P2P payment users somewhat or strongly agree that they feel fully informed about the potential risks of using P2P payment apps. Only 6 percent of P2P payment users strongly agree that they feel fully informed.
- Nearly 3 in 10 P2P payment users (29 percent) said they feel “not too” or “not at all” knowledgeable about how to use the P2P payment service they use most often.

Finding 7, in the Key Findings section of this report, focuses on broad transparency concerns that were raised throughout this research project.

Industry Overview

Since the COVID-19 pandemic began, consumers have been increasingly using digital methods to make payments. As part of Consumer Reports' look into fintech and P2P payments, we engaged consumers in several nationally representative surveys over the course of 2022. In August, we found that 83 percent of Americans—and 90 percent of Americans under age 60—were using at least one fintech app on their mobile devices, and that Americans were using an average of two of the types of fintech apps we asked about. The most popular types of fintech apps are banking apps, payment apps, and digital wallets, in that order.[8]

P2P payment services in particular are deeply integrated into consumer life in the U.S. Well over half of Americans (64 percent) use a P2P payment app for payments to and from other individuals (not businesses), including 4 out of 5 (81 percent) of the 18-to-29 age group, according to our March survey. Two out of 5 Americans (40 percent) said they use P2P payment services at least once a month; nearly 1 in 5 (18 percent) use them at least once a week.[9] As of 2022, there are almost 150 million P2P payment app users in the U.S., representing nearly 62 percent of all mobile phone users 14 and older.[10] The value of P2P payment app user transactions now totals almost $1.1 trillion per year, and is expected to double by 2026.[11]

While P2P payment apps have proved to be popular, users can encounter problems that can put their money at risk. A CR survey in March 2022 found that of those who use P2P payment services at least once per week, 12 percent said they had sent money to the wrong person and 9 percent said they had been the victim of a scam.[12]

CR also reviewed the laws, regulations, and academic literature relevant to P2P apps, which can be found in Appendix 2.

[8] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,123 U.S. adults, August 2022.
[9] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,116 U.S. adults, March 2022.
[10] Toplin, 2022.
[11] Ibid.
[12] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,116 U.S. adults, March 2022.

Key Findings

Finding 1: Policies for resolving fraud and errors can leave consumers at risk of losing money.

None of the four apps—Apple Cash, Cash App, Venmo, or Zelle—sufficiently reimburse customers in the case of unauthorized transactions, such as induced fraud. Although Venmo says it will fully compensate users for all unauthorized transactions, it specifies, for example, that user-initiated authorizations that exceed the initial authorization are not covered unless the user notifies Venmo and specifically rescinds the authorization. Users of the other three services, by contrast, may be liable for up to $50 if an unauthorized transaction is reported within a certain—in some cases very short—time frame. If the unauthorized transaction is reported after that time frame, users may be liable for up to $500. These liability limits follow Regulation E,[13] which caps consumer liability in the event of unauthorized transactions.[14] Regulation E defines "timely notice" as "two business days after learning of the loss or theft of the access device."

Accidentally sending money to the wrong person, often through a minor mistake like a typo in the recipient's user name, is a common problem for consumers.[15] In that circumstance the money is generally not recoverable except at the discretion of the person who accidentally received it. P2P payment companies' often instruct their users to make sure they are sending to the right person before they hit the "send" button. Consumers try their best, with about two-thirds of P2P payment users (66 percent) reporting that they always check to make sure it's the right person when sending money to someone for the first time, and over a third (39 percent) reporting that they always check even when it's someone they've previously sent money to, according to a recent nationally representative CR survey.[16] But increased protections are clearly needed.

Table 1: Fund Protection—Unauthorized Transactions

[13] Regulation E (Part 1005—Electronic Fund Transfers) implements the Electronic Fund Transfer Act (EFTA, 15 U.S. Code § 1693a), which establishes a basic framework of the rights, liabilities, and responsibilities of participants in the electronic fund and remittance transfer systems.
[14] EFTA and Regulation E distinguish between unauthorized transactions, which includes cases of fraud, and errors, which includes cases where a user accidentally sends funds to the wrong person. In both categories, consumers mostly bear the burden to avoid fraud and resolve errors.
[15] www.nbcnews.com/better/lifestyle/use-payment-apps-venmo-zelle-cashapp-here-s-how-protect-ncna1015851.
[16] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,519 U.S. adults, September 2022.

Venmo	If a consumer notifies Venmo within 60 days of the statement, Venmo will fully cover all unauthorized transactions.
Cash App	If a person reports an unauthorized transaction within two business days of learning about the unauthorized transaction, their potential loss will be capped at $50. If the report occurs after two days, the terms state that a person could lose as much as $500. If the person does not report an unauthorized transaction within 60 days of the statement being sent, the person may not be able to recover any funds.
Zelle	If a person loses their device or if their password is compromised and they notify Zelle within four days of learning of the incident, user liability will be capped at $50. If a person waits longer than four days, they could potentially be liable for up to $500.
Apple Cash	Customers have 60 days from the date a statement was issued or the date they electronically accessed payment account information to report an error. The policy states that error reports will be investigated in 10 business days, and results of the investigation will be shared within three business days of the completion of the investigation. If a person reports an unauthorized transaction within two business days of learning about the transaction, losses will not exceed $50. If a person waits more than two days to report the unauthorized transaction, they can lose up to $500.

Finding 2: P2P payment apps collect large amounts of consumer data, may share the data with other companies, and often make it difficult for consumers to delete the data.

A recent Consumer Reports survey found that 65 percent of Americans are "somewhat concerned" or "very concerned" about how much data financial apps collect and store about their users.[17] As we have noted in prior investigations, many financial apps collect large amounts of personal data, which could compromise privacy and lead to security risks.[18] Although some banks have begun giving their customers tools to safely connect to these apps and control what data are shared, P2P payment apps disclose that they could collect and store a tremendous amount of data on their users, in a variety of ways, including the following:

- Identifying information that users provide at sign-up;
- Data on the consumer's use of the service, including the amounts, dates, and recipients of payments;
- Data from the user's mobile device, such as contacts, location data, the network being used, and even fingerprints;
- Data on the user's web activity, which is collected using cookies and other automated tracking technologies; and
- Data about the user collected from third-party sources, including credit bureaus, financial institutions, and employers.

In short, P2P payment apps appear to collect far more data, and more types of data, than they need to provide the services that consumers expect. All four of the reviewed apps disclose that they could collect personally identifying information, information about the network and device used to access the service, and financial information. Some apps go beyond this and additionally collect consumer health information, profile pictures, network preferences, social media, and email use.

All ascribe various purposes for collecting the data, but only some specify which elements or types of collected data are used for which purposes. Notably, all four apps list their data uses in sometimes vague, open-ended language that could enable them to use the data for any purpose at all. All the apps state that they share data with

[17] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,123 U.S. adults, August 2022.
[18] "Consumers Get More Control Over the Banking Data Shared With Financial Apps," *Consumer Reports,* November 2019.

unnamed third parties. Except for Apple, they have weak data-deletion policies. And it is difficult or impossible for users to delete their own data.

Consumer Reports shared its findings with the four companies and asked each whether they would review their policies to improve transparency around data sharing and usage. Only Cash App explicitly acknowledged the need for greater clarity in this area and committed to work with CR to make it clearer to users how their data is used and shared.

Table 2: Data Collection, Sharing, and Deletion

Venmo	***Data Collection and Usage:*** Venmo's policy states that it can collect many data elements, including multiple device IDs, Social Security number, profile photo, geolocation via GPS, IP address, cell tower triangulation, WiFi hot spot location, contact information, data from connected accounts, and financial information. Venmo can collect "additional information from or about you in other ways not specifically described here." Data uses include improving services, marketing, and "shar[ing] personal information with … affiliates and subsidiaries … but only for ... purposes allowed by this document." ***Data Sharing:*** Documentation states that data are shared with unnamed third-party service providers. Venmo's terms contain overly general descriptions of the types of third parties. For example, they do not differentiate among analytics providers, infrastructure providers, marketing partners, and other types of third parties. ***Data Deletion:*** No description of proactive data deletion practices. No mention of a retention period for user information. Data from people who no longer use Venmo will continue to be shared, and policy does not disclose whether data are deleted when an account closes.
Cash App	***Data Collection and Usage:*** Cash App's documentation says personally identifying information collected includes passport number and driver's license number. The service also collects contact data, including recipients and people in contact lists. Cash App "creates and stores inferences about a person's habits and preferences." Data uses include marketing, product development, and "any other reason we may tell you about from time to time." As noted above, Cash App has committed to work with CR to make it clearer to users how their data is used and shared.

	Data Sharing: Documentation states that data are shared with companies such as BugSnag, an analytics provider; Block, Cash App's parent company; and other unnamed third parties. The policy provides adequate descriptions of the types of companies with which it shares data. Cash App's privacy policy states that it will share data with law enforcement and governments, including in support of a garnishment or lien. ***Data Deletion:*** Cash App maintains a help page that describes a process for deleting an account and personal information. This page offers more detail than the legally binding documentation, but it does not specify the precise data that are deleted or whether any data are retained by Cash App after a person deletes their account. Cash App's privacy policy states that it will keep user data "as long as reasonably necessary" and will retain data after a person has deactivated their account. The privacy policy does not appear to describe how data will be treated if a person closes or deletes their account permanently.
Zelle	***Data Collection and Usage:*** Zelle's documentation states that it can collect contact lists if the user consents, and data related to cross-device tracking. Zelle collects user personal information from unspecified "service providers." Data uses include security, compliance, internal operations, research, development, issue resolution, marketing, and "other one-time uses." ***Data Sharing:*** Policies state that data are shared with law enforcement, government agencies, and other authorized and unnamed third parties. Descriptions of the types of third parties with which Zelle shares data are inadequate. Zelle indicates that it shares data with "service providers" but does not delineate between types of services. ***Data Deletion:*** No description of a data deletion process or a review process to identify unneeded data. No mention of a specific retention period for user information. Zelle's terms state that Zelle will retain data as long as it is necessary and relevant for its operations. Zelle's app privacy policy describes a process whereby users can request to delete their data and close their profile by selecting "Delete Account." This cancels the account and the user's ability to use the service, but selecting "Delete Account" does not guarantee that information related to the account will be deleted, and the policy does not specify how a user would know either way.

Apple Cash

Data Collection and Usage: People using Apple Cash have already purchased at least one Apple product, which means Apple has data about them from that product. Described data uses include fraud prevention and compliance with legal requests. Apple's main privacy policy also states that it can use data for "other purposes" with the user's consent.

Data Sharing: Apple's documentation states that data are shared with unnamed third parties. The policy provides adequate descriptions of the types of third parties with which data are shared, including Apple affiliates, service providers used by Apple, developers, and publishers. Green Dot Bank, the technology platform used by Apple Cash, also describes data sharing affiliates and non-affiliates.

Data Deletion: The policy provides adequate general descriptions about proactively identifying data that can potentially be deleted. It discloses that transaction data can be retained for up to five years, including after an Apple Cash account is closed.

Finding 3: App disclosures and documentation[19] contain vague descriptions of security measures; there may be discrepancies between P2P companies' disclosed security protocols and their practices.

Consumers store highly sensitive financial and personally identifying data in their P2P apps. It could be highly damaging to users if the data were exposed or stolen. As such, P2P payment apps are held to high data security standards. And yet all apps reviewed have often vague and varying descriptions about their use of encryption and other technological data security measures. Greater information should be shared regarding use of encryption and security protocols across all apps, and information, when shared, should be made as plain as possible and located in obvious, easy-to-find places.

Although all of these apps likely maintain Payment Card Industry Data Security Standard compliance—which requires layered security that includes encryption—only Cash App's security page states that Cash App maintains a PCI DSS level 1 certification. However, Cash App Investing—a part of Cash App outside the scope of this investigation—suffered a data breach in December 2021 that affected 8 million people and included the theft of customer names and Cash App brokerage account numbers, as well as more specific information for some users.[20] The incident raises concerns about the platform's data security practices because PCI DSS compliance should have prevented such a breach.

On the consumer end, most P2P payment app users do what little they can to increase their security on the apps. In a recent CR survey, 72 percent of P2P payment app users said their app requires identity verification. And more than 1 in 3 users (37 percent) said they had actively tried to increase their security on the app by turning on identity verification settings.[21]

Even so, P2P payment app users are not overwhelmingly confident about the data security practices of these apps: About a quarter either disagreed that their app adequately protects their payments data from security risks like hacking and identity theft (15 percent), or said they simply didn't know (13 percent).[22]

---

[19] The publicly available documentation we reviewed included terms and conditions, end user license agreements, privacy disclosures, company web/mobile app pages. Herein: documentation.
[20] www.sec.gov/ix?doc=/Archives/edgar/data/1512673/000119312522095215/d343042d8k.htm.
[21] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,519 U.S. adults, September 2022.
[22] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,519 U.S. adults, September 2022.

Table 3: Security Practices	
Venmo	Venmo's privacy policy describes using data encryption as a "computer safeguard." Venmo's safety page states that transactions made using the Venmo app are encrypted. These statements do not clearly define the precise nature of the encryption or limits of what is encrypted.
Cash App	Cash App's documentation does not provide specific details on whether and what data are encrypted via end-to-end encryption. A Cash App help page implies that information sent to Cash App is encrypted in transit. Cash App's security page states that Cash App maintains a PCI DSS level 1 certification, which requires layered security that includes encryption.
Zelle	Zelle's documentation states that data encryption is used to protect information, but it does not state that end-to-end encryption is a feature or whether it is enabled by default. Zelle's legally binding documentation does not include descriptions of a security program, but the privacy policy does list some security measures and safeguards.
Apple Cash	Based on Apple's disclosures in the iCloud security overview and the Apple Pay security and privacy overview, Apple takes steps to ensure that data are encrypted in transit and at rest. Apple also maintains security documentation with detailed information and commitments on hardware, system, and application security, and a page providing security fixes and links to more detailed summaries.

Finding 4: Users must meet sometimes confusing conditions to ensure that their funds are protected by FDIC insurance.

P2P payment app users who keep money in their P2P payment account may believe that their money is federally insured with the same protections they have come to expect from traditional bank accounts. However, our review of app documentation shows that this is often not the case.

With three of the services—Apple Cash, Cash App, and Venmo—users have to meet certain conditions in order for funds held in the app to be eligible for Federal Deposit Insurance Corporation (FDIC) pass-through insurance. (They may need to register their account, for example, or use an additional service or feature provided by the company.) This is not applicable to Zelle, which does not hold user funds.

One CR survey found that a small minority (6 percent) of P2P payment app users fund their P2P payments from a balance they maintain in the app itself, essentially using the app as a bank.[23] Given that the number of consumers using P2P payment apps has grown, and the lack of clarity around how to obtain FDIC insurance in the apps, we suspect a large portion of these funds are uninsured.

This discrepancy between users' beliefs that their funds are insured and the apps' stated policies is concerning, given the increased use of P2P payments by consumers. Users could be hurt financially if the companies behind the apps suffer losses or declare bankruptcy.

Table 4: Fund Protection—Insurance of Funds

Venmo	Venmo's documentation is unclear and contains contradictory statements. In particular, the documentation states that FDIC pass-through insurance is available only if a person has purchased cryptocurrency, or added money via direct deposit or remote check capture. However, later in the policies Venmo states that FDIC pass-through insurance applies only to U.S. dollar funds and not cryptocurrencies, notwithstanding the earlier language.
Cash App	Cash App's documentation states that, by default, funds are not eligible for FDIC pass-through insurance. But if a user chooses to apply for the company's debit card, known as the Cash Card, and

[23] Consumer Reports nationally representative American Experiences Survey (PDF) of 2,116 U.S. adults, March 2022.

	Cash App determines that a person is eligible for the Cash Card, the person's funds held within Cash App are protected with FDIC pass-through insurance through a banking partner. Notably, the app explicitly informs users during the sign-up process that their funds are not FDIC-covered by default and directs them to register for the debit card for coverage.
Zelle	Not applicable. Zelle's terms state that it only facilitates a transfer and therefore does not hold client money.
Apple Cash	Apple's terms and conditions state that money held in the payment account will not be eligible for insurance from the FDIC until the user registers the Apple Cash Account.

Finding 5: The apps make it difficult for users to understand and track updates to legally binding documentation.

CR's review found that it would be very difficult for users to track changes to the legally binding terms governing P2P app policies. For example, because Zelle does not appear to share any archives of past policies, or share any obvious way of tracking differences between policies, the only way for consumers to know what changes are taking place is to archive a copy themselves and regularly check the current policy against their archived version. It's unrealistic for consumers to do that with one policy, let alone multiple policies. Likewise, Cash App considers all notifications to have been received within 24 hours of the date the notification was sent. Even CR's privacy policy researcher, who reviewed the legally binding documentation for this evaluation, stated that they would find it challenging if not impossible to review and fully understand changes in legally binding documentation within 24 hours.

Simply finding the relevant documents can be challenging. For example, Zelle includes language about updates to legally binding terms in *four* different policies: its user service agreement, E-sign disclosure and consent, terms of service, and app privacy notice. Similarly, understanding the specific data collected by Apple requires finding and reading multiple documents stored and linked in different locations on Apple's website, and the complexity of finding these documents is likely beyond the capability of people without specialized training or experience.

All four apps state that using the service after a notice has been sent equates to accepting the updated terms. There's no real option for users if they disagree with any of the terms of the legally binding documentation beyond simply canceling their accounts, which could create problems for their financial lives.

Table 5: Accessible and Transparent Information— Updates to Legally Binding Documentation	
Venmo	Venmo's user agreement states that Venmo can update the agreement at any time for any reason. The user agreement also states that, if the changes reduce consumer rights, users will be given at least 21 days' notice. However, that statement is followed by language stating that Venmo "reserve[s] the right to amend this agreement at any time without notice."
Cash App	Cash App's legally binding documentation states that Cash App will determine what "reasonable" notification entails, and considers

	all notifications to have been received within 24 hours of the date the notification was sent. Additionally, Cash App states that using the service after the terms have been updated equals consent to the updated terms.
Zelle	Zelle includes language about updates to legally binding terms in four different policies: the user service agreement, the E-sign disclosure and consent, the terms of service, and the app privacy notice. In general, Zelle claims the right to change the terms at any time. Users are told that they need to check the policies regularly for updates and that using the service after any change means that the user has accepted the updated terms.
Apple Cash	The Apple Payments and Green Dot Bank terms state that terms can be updated at Apple Payments/Green Dot's discretion. The terms also state that if notification is required, the notification will be sent electronically as defined in the electronic communications agreement. The terms also contain a clause stating that using the service after a notice has been sent equates to accepting the updated terms.

Finding 6: Users are generally required upon sign-up to give up certain legal avenues for resolving potential disputes.

All four apps require that users agree at sign-up that all future legal claims and disputes against the company will be resolved on an individual basis, mostly through binding arbitration. These requirements are especially concerning because, as a 2020 Consumer Reports article put it: "Because arbitration proceedings are private, and because arbitration clauses almost always forbid plaintiffs from joining together, companies can use arbitration to preemptively crush consumer challenges to their practices, no matter how predatory, discriminatory, unsafe—and even illegal—they may be."[24]

Three of the services give users 30 days to opt out of the requirement by mailing a written notice, but it may be unrealistic to expect users to take advantage of this option before disputes arise.

Table 6: Legal Rights

Venmo	Venmo's user agreement contains language requiring people to use binding arbitration and resolve claims and disputes on an individual basis. Users have 30 days after first accepting the terms of the user agreement to opt out of these requirements by mailing a written notice.
Cash App	Cash App's terms of service include a requirement that disputes be resolved on an individual basis, either via arbitration or in small claims court. People have 30 days to opt out of this clause by mailing an opt-out notice. Additionally, Cash App has an informal negotiation requirement that could take 60 days.
Zelle	Zelle's legally binding documentation requires people to use binding arbitration to resolve disputes and forfeit their right to join a class action. Users can opt out of the agreement to arbitrate and the class-action waiver in writing, postmarked within 30 days of accepting Zelle's terms.
Apple Cash	The Apple Payments and Green Dot Bank terms state that if either party opts for arbitration of a dispute, both sides waive their right to

[24] Medintz, Scott. "Forced Arbitration: A Clause for Concern," *Consumer Reports,* January 30, 2020, accessed November 2, 2022, www.consumerreports.org/mandatory-binding-arbitration/forced-arbitration-clause-for-concern.

a trial. The one exception noted in the terms is that claims will be allowed to proceed if a person brings a claim in small claims court. Claims may proceed only on an individual basis. Unlike the other services we reviewed, the Apple Payments and Green Dot Bank terms do not appear to mention an opt-out window.

Finding 7: Consumer disclosures are often difficult to find and read, reflecting a broad concern about transparency.

Across all of the indicators evaluated in this case study and across all the principles that guided the evaluations, Consumer Reports found reasons for concern about a lack of adequate transparency.

While companies often meet their technical disclosure requirements, the information in some instances was either difficult to find or difficult to read. The privacy policy researcher conducting the data collection for this evaluation, for example, said that embedded finance environments, such as a payment app or function within a larger ecosystem, sometimes make it difficult for consumers to access clear, well-written language and to know which disclosures apply. In one instance, a company had five different sets of related and applicable disclosures; all were difficult to find, despite meeting all legal requirements and using clear language.

Thus, while companies generally provide detailed disclosures outlining various data collection, data retention policies, data collection purposes, data sharing practices, and data control, they often stop short of providing a full picture to consumers because all the relevant information is difficult to locate or to read.

Examples of this included:

- **Detailed disclosures including catch-all phrases that appear to grant the company practically unlimited rights.** Venmo's privacy policy, for example, allows for the collection of "additional information in other ways not described in the privacy policy and user agreement." Zelle's policy uses the phrase: "other one time uses."
- **Inconsistent and insufficient detail about the nature of third-party and partner information sharing.** For example, although Cash App clearly states in its privacy policy that it collects and shares information for various purposes, the policy does not specify whether the third parties are integral to service provision or if the information is shared for the purpose of marketing or advertising.
- **Inconsistent and insufficient detail about whether data sharing also includes sale of data to third parties or targeted advertising.** Only one company, Apple, explicitly states that it does not sell data to third parties. Zelle and Cash App are vague on the subject. Venmo does state that information collected may be used for advertising, but it doesn't use the phrase "targeted

advertising." But because the privacy policy says geolocation and other data can be used for advertising, we suspect the data are used for targeted advertising.

- **Conflation of data and information required for safe use of the service with information not required to use the service.** For example, Venmo's privacy policy states that "[w]e also may collect Geolocation Information (defined below). If you do not agree to our collection of this information, you may not be able to use our Service."

This frequently raised questions: What is meaningful disclosure?

- Do these documentations timely situate consumers with respect to their rights, obligations, expected services, and resources?
- Even if not engaged during the app setup process, is documentation easy to identify and locate? Is the language accessible?
- Is the language used in documentation specific enough to convey desired meaning?

Ratings of Evaluated P2P Payment Services

After evaluating these four P2P payment services and reaching the above findings, we took the next step and rated each service based on the results of our evaluation. While the findings detailed above represent our conclusions after examination, the ratings incorporated several specific sub-principles from the larger Fair Digital Finance Framework.

In these evaluation-based ratings of P2P payment services, CR rated Apple Cash highest for the evaluated indicators across all three principles—safety, privacy, and transparency. Overall, the four services performed notably less well in the transparency principle, driven in part by lower scores for incident notification and providing actionable legal rights. We rated each of the four services good enough to use. The ratings are visualized below.

	WORSE ⟵ BETTER	Apple Cash	Cash App	Venmo	Zelle
Safety	Maximum fund protection	⏫	⏫	⏫	⏫
	Good security practices	⏫	⏫	🔼	🔼
Privacy	Data usage	⏫	🔼	🔼	🔼
	Data collection	⏫	⏫	⏫	⏫
	Minimal data collection	⏫	⏫	⏬	➖
	Data sharing	⏫	⏫	⏫	🔼
	Data deletion	🔼	🔽	⏬	⏬

Transparency	Accessible and transparent information				
	Incident notification				
	Provides actionable legal rights				

GUIDE TO THE RATINGS

Ratings are based on analyses of operational and data policies of mobile versions of peer-to-peer payment services performed by Consumer Reports between August and October 2022.

Safety: **Maximum fund protection** evaluates disclosure of funds' protection, insurance, and return in the case of bankruptcy or sale; monitoring for, notifying users of, and process for handling suspicious or fraudulent activity; and protecting users from and educating users about fraud and scams. **Good security practices** evaluates authentication systems; disclosure of the use of encryption; protection from known software vulnerabilities; protecting user data, including limiting employee access to data, performing or commissioning security audits, and accountable use of third-party contractors; software updates; and addressing reports of vulnerabilities.

Privacy: **Data usage** evaluates whether users can see their data, including downloading a copy of data at no charge and a right to review and correct data, and transparent data usage and data usage that is limited to the initial use for which it was collected. **Data collection** evaluates disclosure of specific data elements collected, how data elements are collected, and the purpose for collecting each type of user data. **Minimal data collection** evaluates whether the data collected are necessary for service provision. **Data sharing** evaluates disclosure of what information is shared with whom and for what purpose. **Data deletion** evaluates disclosure of data deletion processes.

Transparency: **Accessible and transparent information** evaluates disclosure of legally binding documentation, including data collection, user data rights, security practices, explanation of services, and use of machine learning and artificial intelligence. **Incident notification** evaluates disclosure of notification and responses to cybersecurity incidents. **Provides actionable legal rights** evaluates whether users have to give up legal rights to use the service.

Recommendations

In recent years, Consumer Reports has urged policymakers to ensure that all P2P payment companies a) adopt a data minimization approach (i.e., collect and store only necessary information); b) take the most aggressive measures to secure consumer information; and c) aggressively manage fraud and error resolution.[25] Consumer

[25] To deal with some of these issues, Congress proposed the Protecting Consumers From Payment Scams Act for discussion, which would amend the Electronic Fund Transfer Act. This act would treat fraudulently induced electronic fund transfers in the same manner as unauthorized electronic fund transfers. Consumer Reports supports such amendments.

Reports also advocates for responsible innovation. Given that regulation often lags behind innovation, we urge companies to not wait for regulatory clarity in areas where there are clear consumer benefits to maximum safety, privacy, and transparency. A strong stance in support of customer interests should build consumer trust and loyalty and enhance a company's reputation, customer acquisition, customer retention, and customer satisfaction.

In applying the Fair Digital Finance Framework to evaluate peer-to-peer payment products, Consumer Reports has identified the following opportunities to improve products and services, and minimize risk for consumers.

Consumer Safety

Consumer safety encompasses the protection of both user information and client funds. We recommend the following actions for P2P payment firms.

- *Ensure maximum security:* Clearly state which security protocols they use to protect client information. Companies could, for example, maintain a PCI DSS level 1 certification with financial information encrypted in transit and at rest.
- *Ensure maximum fund protection*: Be meaningfully transparent about the availability of FDIC insurance by providing clearer explanations of reimbursement policies in the case of fraud or error. Specifically, go beyond obligations to investigate and resolve fraud under Regulation E of the Electronic Fund Transfer Act (EFTA).[26] In addition, P2P payment firms should publish aggregate data on the level and amount of fraud on their platforms on a regular and frequent basis.

Privacy

Privacy encompasses data collection, data sharing, and data deletion practices. Companies could go beyond disclosing current practices to consumers on a take-it-or-leave-it basis. Under this principle, we recommend the following actions for P2P payment firms.

- *Ensure minimum data collection*: Collect only data required for the prevention of fraud and for provision of the service. Disclose the types of data collected for such purposes in consumer-facing, legally binding terms and conditions.
- *Ensure minimum data sharing*: Identify the individual firms and types of firms with whom they share consumer data, as well as the purpose of such sharing.

[26] "Error Resolution for P2P Payment Services: Beyond the CFPB FAQs," *The Clearing House,* September 2022.

- *Ensure maximum data deletion*: Allow users to see their personal data and delete it if they no longer want to use the service or if the data is not necessary to render the service. Instructions for deleting one's data should be clear and easy to access.

Transparency

Transparency encompasses clear and accessible information about company operations and revenue, and about how to use the service and its features and options. It also includes the consumer's ability to understand all legally binding terms and to exercise their full legal rights if a dispute over the service arises. Under this principle, we recommend the following actions for P2P payment firms.

- *Ensure actionable legal rights:* Do not require that users use binding arbitration or resolve claims on an individual basis.
- *Provide accessible and transparent information:* Provide clear consumer-facing information about the intended use and the associated risks of the service, including important elements such as whether funds are FDIC-insured, what user data are collected and shared, and how users can delete their data. Consumers should also know clearly what remedies are available in the case of unauthorized or erroneous transactions.
- *Ensure incident notification:* Commit to providing real-time notification of service disruptions and to transparently communicating about cybersecurity incidents.

Conclusion

Consumer Reports' evaluation has identified the following app policies or features that could be improved to ensure greater safety, privacy, and transparency protections for consumers:

- None of the apps specify what security protocols are in place and, despite many users' expectations, do not clearly specify whether user funds are FDIC-insured.
- P2P payment apps collect an enormous amount of data from users, share it with a vaguely defined set of partners, and make it difficult for users to delete their information when they stop using the service.
- Consumer disclosures are often difficult to find and read, reflecting a broad concern about transparency.
- All of the apps make it challenging for users to track changes to the legally binding terms of service and require users to sign away their legal rights and use only arbitration to resolve disputes.

P2P payment providers can raise the bar for consumer protection by adopting stronger policies and safeguards that minimize the potential risks for users. CR recommends that providers take the following steps, which would benefit consumers and help establish a new industry standard for fair digital finance:

- State clearly which security protocols they use to protect users' information.
- Be transparent about the availability of FDIC insurance, and clearly explain policies for reimbursing users in cases of fraud or error.
- Collect only the data needed to prevent fraud and provide the payment service. Disclose the data they collect in consumer-facing, legally binding terms and conditions.
- Identify the individual firms and types of firms they share consumer data with and the purpose for sharing the data.
- Allow users to see their personal data and delete it if they no longer want to use the service or if it's not needed to render the service.
- Do not require users to agree to binding arbitration to resolve disputes or resolve claims on an individual basis.
- Provide clear consumer-facing information about the use and risks of the service, including whether funds are FDIC-insured, what user data are collected and

shared, how users can delete their data, and what remedies are available for unauthorized or erroneous transactions.

We look forward to working with all stakeholders in the financial ecosystem to ensure that P2P payment and other fintech products have adequate consumer protections.

Acknowledgments

Consumer Reports' Financial Fairness initiative is supported by a host of staff members across the organization. We would like to thank the following people for their contributions to this report: Delicia Hand, Stephanie Landry, Bill Fitzgerald, Noemi Altman, Ajmal Ahmady, Scott Medintz, Glen Rockford, Maria Rerecich, Tracy Anderman, Michael McCauley, Chuck Bell, Sharee McKenzie Taylor, Jen Shecter, Shar Taylor, Johnny Mathias, David Butler, Camille Calman, and Wendy Greenfield. Jane Manweiler and Tess Yanisch contributed survey research, and Chris Griggs provided design support.

Consumer Reports' investigation of P2P payment apps is part of a broader initiative to monitor, evaluate, and strengthen consumer protections in the burgeoning digital finance marketplace, work that is made possible, in part, by a grant from Flourish Ventures' fund at the Silicon Valley Community Foundation.

We thank everyone for their support of this work.

Appendix 1: Service Overview

Apple Cash

- Launched in 2017.
- Component of the iPhone wallet and can be used to pay for goods and make peer-to-peer transfers.
- There is no publicly available data regarding the number of Apple Cash users or its aggregate transaction value.

Cash App

- Launched in 2013.[27]
- 49 million users as of 2022.[28]
- Owned by Block.
- Total value of transactions on Cash App was expected to reach $116.14 billion in 2022, and is projected to reach $233.82 billion by 2026.[29]
- Cash App began offering crypto trading in 2017 and offers integrated buy now, pay later services since its parent company's 2022 acquisition of Afterpay.

Venmo

- Founded in 2009.
- Estimated 77.7 million users as of 2022.[30]
- Owned by PayPal since 2013, it helped popularize P2P payments.
- Sixteen percent of U.S. adults who use a digital payment platform say Venmo is their primary digital wallet.[31]
- Total value of P2P payment transactions increased from $95.54 billion in 2019 to $282.44 billion in 2022 and is projected to increase to around $540 billion by 2026.[32]

Zelle

- Launched in 2017.
- 61.6 million users as of 2022.[33]

[27] squareup.com/us/en/press/introducing-cashtags.
[28] Cash App November 2022 Investor Earnings Call.
[29] Toplin, 2022.
[30] Toplin, 2022.
[31] CivicScience, civicscience.com/paypal-leads-among-digital-wallet-adoption-but-cash-stays-relevant, 2022.
[32] Toplin, 2022.
[33] Toplin, 2022.

- Owned by Early Warning Systems, which is owned by seven of the largest banks in the U.S. Zelle is both integrated into participating bank and credit unions' mobile banking apps and available as a stand-alone app.
- Zelle has fewer users than Venmo, but the total transaction value on Zelle is almost twice as large as that on Venmo.[34]
- Payment transactions on Zelle increased from $147.54 billion in 2019 to $531.01 billion in 2022 and are projected to grow to $1.17 trillion by 2026.[35]

[34] Based on data from Toplin. Zelle ($531.01 billion in payments with user base of 61.6 million) vs. Venmo ($282.44 billion in payments with user base of 77.7 million), 2022.
[35] Toplin, 2022.

Appendix 2: Legal and Regulatory Overview and Literature Review

Legal Overview

The most pertinent regulation governing P2P payment services is Regulation E (Part 1005—Electronic Fund Transfers), Chapter 10 (Consumer Financial Protection Bureau) of Title 12 (Banks and Banking).[36] These regulations cover all relevant areas, from disclosure requirements to procedures for resolving errors. An FAQ on the CFPB website says P2P payments are considered EFT transactions.[37]

Additional laws and regulations that touch upon electronic payments include the following.

- The Dodd-Frank Act added the concept of abusive practices to unfair or deceptive ones and gave the Consumer Financial Protection Bureau the authority to further define abusiveness.
- The Gramm-Leach-Bliley Act is applied in nonbank mobile payments where the provider will diverge from with the model. It should also be applicable to mobile payment entities and is applicable to providers involved in more traditional payment channels. The GLBA requires such institutions to explain information-sharing practices to their customers and to safeguard sensitive data.
- Relevant anti-money-laundering requirements are stipulated in the Bank Secrecy Act. The BSA provides rules governing “know your customer” requirements.
- State laws also may govern the activity of nondepository money services and fund transfer providers such as check cashers, currency dealers, and money transmitters.[38]

The Consumer Financial Protection Act gives the CFPB the authority to standardize nonbank providers of consumer financial products and services. The financial products include extending credit and issuing stored value or payment instruments, which provide payment or other financial information processing products. They also include the payments made via online banking or by means of a mobile telecommunication network.

---

[36] Congress “Electronic Fund Transfer Act,” 15 USC 1693 et seq., Washington, D.C., October 14, 1978.
[37] “Regulation E Frequently Asked Questions,” *Consumer Financial Protection Bureau,* CFPB website, Washington, D.C., December 13, 2021.
[38] BCC Research staff, “Mobile Wallet and Payment Technologies: Global Markets,” *BCC Research,* Report Code: FIN002A, 34, April 2019.

Literature Review

Consumer Reports reviewed industry and academic papers related to P2P payment transaction markets. These papers generally provide evidence of the sector's increasing importance as the number of users and transaction value increase, identify measurable impacts on user behaviors, and point to security and privacy risks associated with P2P payment services. Some of the relevant literature is summarized below.

Industry Reports

- Insider Intelligence's May 2022 report provides helpful historical and projected P2P payment user numbers and transaction volumes for the industry as a whole, as well as growth dynamics for the largest players in the industry.
- BCC Research (2019) provides a review of global market trends, as well as regulatory issues. The Business Research Company (2022) provides a review of global lending and payments markets, and Forrester (2018) provides an overview of the future of payments.

Academic Reports

- Greene et al. (2022) reviewed consumers' preferred payment methods for paying other individuals and found that while cash still is preferred for small-value transactions, approximately 94 percent of consumers rank electronic technologies as their second preference.
- Tetyana Balyuk (2021) uses Zelle transaction data and concludes that the P2P payment system is beneficial, with Zelle use resulting in fewer overdrafts and higher consumption by financially fragile consumers. Diniz et al. (2011) provide a helpful review of existing P2P payment literature to the date of the paper's publication. More broadly, in terms of regulation, Katz (2015) in the Berkeley Technology Law Journal reviews regulatory approaches for P2P payment marketplaces.
- Li et al. (2021) explore the influences of using digital P2P payments on people's experiences of interpersonal financial exchanges and their offline interpersonal relationships. They find several measurable social impacts, including that using digital P2P payments helps reduce awkwardness and ensures a stronger sense of fairness in financial exchanges. In addition, though digital P2P payments can relieve tension and reduce distrust in users' interpersonal relationships, they also result in loss of emotion and increased peer pressure.
- Sahi et al. (2022) review the rapidly increasing literature on privacy and security risk of digital payments. They review 591 existing studies and find that academic research thus far has focused on perceived privacy and security, and has not

considered the relationship between risk attributes. The paper provides suggestions to improve digital payment research in the future.

- The Federal Reserve Bank of Atlanta (Windh, 2011) provides a survey of the P2P payment landscape from a decade ago. More recently, the Federal Reserve Bank of Kansas City (Bradford, 2017) reviewed the growth of the sector and concluded that bank-provided services "may soon go toe-to-toe with nonbank-provided services."
- Belanche et al. (2022) review the growth and success factors of P2P payment provider Bizum in Spain, and conclude that age and gender do not significantly influence adoption, which suggests that the service might be used by a wide spectrum of users.

Appendix 3: Testing Scope

Because one of the key goals of this study is to evaluate the performance of the draft Fair Digital Finance Framework while we were also evaluating products, maintaining feature parity across the services was required to minimize noise in the raw test results. Maintaining feature parity also allowed us to isolate and test a common foundation for all users accessing these services. The following notes detail some of the specifics of this process.

Apple Pay/Cash

Testing for peer-to-peer transactions using Apple's offerings involves multiple services from Apple, including Wallet, Messages, Apple Pay, and Apple Cash. While the specific service that facilitates the transaction is Apple Cash, the various services have interdependent features: For example, a peer-to-peer transfer via Apple Cash can be initiated via either Messages or Wallet. Additionally, the terms for Apple Cash explicitly state that Apple Pay must be enabled in order to use Apple Cash. Features not directly related to supporting peer-to-peer transfers (such as storing a student ID or a transit pass in Wallet, or paying via a credit card in Apple Pay) are not in scope for testing. As with other services, testing was focused on the elements used to support a person transferring money to or receiving money from another person.

Cash App

Cash App has a debit card option, an investing option, and a business option. These items are not in scope, as they all fall outside the core service of a person transferring money to another person or receiving it from another person.

Cash App also has legacy terms for people who signed up before June 24, 2021, and have not accepted the new privacy notice. Because there is no clear way to tell how many people (if any) are governed by these terms, and because all of the other services are evaluated based on their current terms, the legacy terms are not in scope and were not used in testing.

Venmo

Venmo has multiple features in addition to peer-to-peer payments; an incomplete list includes direct deposit, crypto trading, and a Venmo credit card. These features, and their privacy and security implications, are out of scope for this testing. As with the other services under test, this initial test focuses on the core service of a person transferring money to another person or receiving it from another person.

Zelle

Zelle is bundled within services offered by many banks and is also available as a standalone app. When Zelle is offered through a bank, in general, the terms of service and privacy practices of the bank affect how Zelle can use or access data. Our testing looked at the use case of a person using Zelle as a standalone app, not as a service offered by a bank.

Appendix 4: Bibliography

Apple (2022). Legal Terms and Relevant Other Documents:

Legal Terms

General Policies

- Apple's main privacy policy: www.apple.com/legal/privacy/en-ww.
- Privacy labels (Apple Wallet and Messages): www.apple.com/privacy/labels.
- Government information requests: www.apple.com/privacy/government-information-requests.
- iCloud security overview: support.apple.com/en-us/HT202303.

Apple Cash Policies[39]

- Apple Cash (Green Dot Bank privacy policy): applecash.greendot.com/privacy (October 2, 2017).
- Apple Cash and Green Dot Bank terms and conditions (August 5, 2021), and electronic communications agreement (August 6, 2019): applecash.greendot.com/termsconditions (called "Apple Payments and Green Dot Bank Terms").
- Apple Cash and Apple Payments privacy information: www.apple.com/legal/privacy/data/en/apple-cash-apple-payments-inc (August 6, 2019).

Apple Pay[40]

- Apple Pay and privacy: www.apple.com/legal/privacy/data/en/apple-pay (September 12, 2022).

Apple Wallet

- Apple Wallet and privacy: www.apple.com/legal/privacy/data/en/wallet.

Other Relevant Documents

- Apple Pay overview: support.apple.com/apple-pay.
- Apple Pay security and privacy overview: support.apple.com/en-us/HT203027 (this page contains language and text links that blur the lines between Apple Pay and Apple Cash).

[39] Note: Apple Payments is not the same as Apple Pay; Apple Cash card is not the same as Apple Card.
[40] Testing uses the terms shared at applecash.greendot.com/termsconditions.

- Updating cards in Apple Pay: support.apple.com/en-us/HT205583.
- Set up Apple Cash: support.apple.com/en-us/HT207886.
- Add money to Apple Cash: support.apple.com/en-us/HT207881.
- Send and receive money with Apple Cash: support.apple.com/en-us/HT207875.
- An additional support page for Apple Cash: support.apple.com/guide/iphone/use-apple-cash-iph385cf0980/ios.
- Links to privacy overview pages for more than 80 Apple services: www.apple.com/legal/privacy/data.
- Apple Cash overview: support.apple.com/apple-cash.
- Set up Apple Pay: support.apple.com/en-us/HT204506.
- Close Apple Cash: support.apple.com/en-us/HT207883.
- Apple Wallet privacy and security overview: support.apple.com/en-us/HT213046.
- Apple Wallet overview in the iOS 16 documentation: support.apple.com/guide/iphone/keep-cards-and-passes-in-wallet-iphc05dba539/ios.
- Apple Cash security: support.apple.com/guide/security/apple-cash-security-sec133775d09.
- Avoid scams support page: support.apple.com/en-us/HT208226.
- If your Apple Cash account is locked: support.apple.com/en-us/HT207932.
- Security Bounty page: developer.apple.com/security-bounty.
- Security Bounty terms of service: developer.apple.com/security-bounty/requirements.
- Report a security issue: support.apple.com/en-us/HT201220.
- Apple privacy rights page: support.apple.com/en-us/HT208501.
- Apple security updates: support.apple.com/en-us/HT201222.
- Apple platform security overview: support.apple.com/guide/security/intro-to-apple-platform-security-seccd5016d31 (has information on security reviews, etc.).
- Delete Apple ID: support.apple.com/en-us/HT208504.
- California privacy rights, general overview: www.apple.com/legal/privacy/california.
- Detailed disclosures in response to California privacy rights (43 services): www.apple.com/legal/privacy/california/ca-privacy-disclosures.html.
- Full details on getting a copy of data associated with Apple ID: support.apple.com/en-us/HT208502.

- Transparency report: www.apple.com/legal/transparency.

iOS Safety Information

- Activate Lost Mode: support.apple.com/guide/icloud/use-lost-mode-mmfc0f0165/icloud.
- Erase a device: support.apple.com/guide/icloud/erase-a-device-mmfc0ef36f/icloud.
- Face ID: support.apple.com/en-us/HT208109.
- Touch ID: support.apple.com/en-us/HT201371.
- Passcode: support.apple.com/en-us/HT204060.
- iPhone updates: support.apple.com/en-us/HT204204.
- Security reports: support.apple.com/en-us/HT201220.

Apps

- Google Play: N/A.
- App Store: apps.apple.com/us/app/apple-wallet/id1160481993.

Balyuk, T. & Williams, E., "Friends and Family Money: P2P Transfers and Financially Fragile Consumers," Harvard Business School, Boston (November 2021), www.hbs.edu/ris/Publication Files/Friends and Family Money_EW_070667a7-ea14-40d6-a6da-9a117abbd358.pdf (PDF; accessed September 19, 2022).

BCC Research staff, "Mobile Wallet and Payment Technologies: Global Markets," Report Code: FIN002A (April 2019).

Belanche, D., Guinaliu, M. & Albas, P., "Customer adoption of p2p mobile payment systems: The role of perceived risk," Telematics and Informatics Journal, Zaragoza, Spain (June 10, 2022).

Bradford, T., "Banks Re-enter the P2P Payments Fray: With Mobile, Will this Time Be Different?" Federal Reserve Bank of Kansas City, Mo. (January 2017).

Business Research Company, "Lending and Payments Market: Global Briefing 2022," United Kingdom (May 2022).

Caceres-Santamaria, A., "Peer-to-Peer (P2P) Payment Services," Federal Reserve Bank of St. Louis, Economic Research,

research.stlouisfed.org/publications/page1-econ/2020/04/01/peer-to-peer-p2p-payment-services (accessed September 8, 2022).

Cash App (2022). Legal Terms and Relevant Other Documents:

Legal Terms

- Privacy policy: cash.app/legal/us/en-us/privacy (effective/updated January 26, 2022).
- Terms of service: cash.app/legal/us/en-us/tos (updated Aug, 19, 2022).
- Cash App acceptable use policy: cash.app/legal/us/en-us/acceptable-use-policy (updated May 16, 2022).
- E-sign consent: cash.app/legal/us/en-us/sign (updated December 10, 2021).
- Privacy notice : appears to be the same as the privacy policy, but at a different URL, cash.app/legal/us/en-us/privacy-notice.

Other Relevant Documents

- Uptime status page: status.cash.app and status.cash.app/history.
- Security page: cash.app/security.
- Scam protection/safety page: cash.app/help/ua/en-us/3127-keeping-your-cash-app-secure.
- Recognize scams: cash.app/help/us/en-us/6482-recognize-scams.
- Bitcoin promo page: cash.app/bitcoin.
- General help options: cash.app/help.
- Contact page (multiple options): cash.app/contact.
- Help page about locked accounts: cash.app/help/us/en-us/3129-locked-account.
- Bugcrowd page: bugcrowd.com/cashapp (found via search; not linked on the Cash App site).
- Help page on how to delete your personal information: cash.app/help/US/EN-US/6498-delete-personal-information.
- Careers page: cash.app/careers.

Apps

- Google Play: play.google.com/store/apps/details?id=com.squareup.cash (updated August 22, 2022).
- App Store: apps.apple.com/us/app/cash-app/id711923939 (version 3.7.2; updated August 22, 2022).

Consumer Financial Protection Bureau, "Regulation E Frequently Asked Questions," CFPB website, Washington, D.C. (December 13, 2021).

Congress, "Electronic Fund Transfer Act," 15 USC 1693 et seq., Washington, D.C. (October 14, 1978).

Congress, "Amendment of Electronic Fund Transfer Act," 117th Congress 2nd Session, Washington, D.C. (2021).

Consumer Reports, "Peer-to-Peer Payments Are Generally Safe, But Consumers Must Be Aware of Risks," Washington, D.C. (August 2018).

Consumer Reports, "Why Apple Pay Is the Highest-Rated Mobile P2P Payment Service," Washington, D.C. (November 2018).

Consumer Reports, "Peer-to-Peer Payment Apps: A Digital Standard Case Study," Washington, D.C. (August 2020).

Consumer Reports, "Why P2P Payment Apps Aren't as Safe as Credit Cards," Washington, D.C. (January 2021).

Consumer Reports, "The Truth About Those Peer-to-Peer Payment Apps," Washington, D.C. (April 2022).

Consumer Reports, "Do This One Thing to Protect Your Peer-to-Peer Payments," Washington, D.C. (May 2022).

Crowe, M., McGuire, B. & Tavilla, E., "Results from the 2019 Federal Reserve Mobile Financial Services Survey of Financial Institutions," Federal Reserve Bank of Boston (December 23, 2019).

Diniz, E., Albuquerque, J. & Cernev, A., "Mobile Money and Payment: a literature review based on academic and practitioner-oriented publications (2001-2011)," GlobDev 2011: Proceedings Annual Workshop of the AIS Special Interest Group for ICT in Global Development (December 3, 2011).

Duarte, J., Siegel, S. & Young, L., "Trust and Credit: The Role of Appearance of P2P Lending," The Review of Financial Studies, Vol. 25, No. 8 (August 2012), pp. 2,455-2,483.

Forrester Research, “The Future of Payments” (2018).

Greene, C., Prescott, B. & Shy, O., “How people pay each other: Data, theory, and calibrations,” Journal of Behavioral and Experimental Economics, Vol. 96, ISSN 2214-8043 (February 2022).

Harkness, S., “Discrimination in Lending Markets,” Social Psychology Quarterly, Vol. 79, No. 1 (March 2016), pp. 81-93.

Herzenstein, M., “The Role of Narratives in P2P Lending Decisions,” Journal of Marketing Research, Vol. 48, Special Interdisciplinary Issue 2011: Consumer Financial Decision Making (2011), pp. S138-S149.

Katz V., “Regulating the Shared Economy,” Berkeley Technology Law Journal, Vol. 30, No. 4, Annual Review (2015), pp. 1,067- 1,126.

Kalinic, Z. et al., “The moderating impact of gender on the acceptance of peer-to-peer mobile payment systems,” International Journal of Bank Marketing, ISSN: 0265-2323 (July 25, 2019).

Li, L., Freeman, G. & Wohn, D., “The Interplay of Financial Exchanges and Offline Interpersonal Relationships through Digital Peer-to-Peer Payments,” Telematics and Informatics, Vol. 63 (October 10, 2021).

Ma, L., Wang, Y., Ren, C., Li, H. & Li, Y. (2020). “Early Warning for Internet Finance Industry Risk,” Journal of Coastal Research, Special Issue No. 106, Advances in Coastal Research: Engineering, Industry, Economy, and Sustainable Development (Summer 2020), pp. 295-299.

Pope, D. & Sydnor, J., “Evidence of Discrimination from Prosper.com,” The Journal of Human Resources, Vol. 46, No. 1 (Winter 2011), pp. 53-92.

Sahi, A. et al., “The Research Trend of Security and Privacy in Digital Payment,” Informatics Journal, Basil, Switzerland (April 6, 2022).

Toplin, J., “US Mobile Peer-to-Peer Payments Forecast 2022,” Insider Intelligence.

Venmo (2022). Legal Terms and Relevant Other Documents:

Legal Terms

- Privacy policy: venmo.com/legal/us-privacy-policy (February 28, 2022).
- Acceptable use policy: www.paypal.com/us/legalhub/acceptableuse-full (September 21, 2021).
- E-sign consent: venmo.com/legal/us-consent (undated).
- User agreement: venmo.com/legal/us-user-agreement (May 23, 2022).
- Payment method rights: venmo.com/legal/us-payment-method-rights (undated).

Other Relevant Documents

- Fees: venmo.com/resources/our-fees.
- Trust and safety page: venmo.com/about/us/trust-and-safety.
- Accessibility: venmo.com/accessibility.
- Common scams on Venmo: help.venmo.com/hc/en-us/articles/360048404533-Common-Scams-on-Venmo (surfaced via focused search).
- Log-in security, including text-based two-factor authentication: help.venmo.com/hc/en-us/articles/217532397 (surfaced via focused search).
- Pin ID: help.venmo.com/hc/en-us/articles/217532257-PIN-Touch-ID (surfaced via search).
- Law enforcement reports: safetyhub.paypal.com (portal for handling law enforcement data requests).
- Global investigations team: www.paypal.com/us/webapps/mpp/law-enforcement (starting place for governments and law enforcement agencies to get data from PayPal).
- Unfreeze account page: help.venmo.com/hc/en-us/articles/217532077-Temporarily-Frozen-Account-from-Failed-Payments (uncovered via search for “security audit”).
- Security help page: help.venmo.com/hc/en-us/articles/360035844973-Security (surfaced via a focused search for “security audit”).
- Venmo privacy settings help page: help.venmo.com/hc/en-us/articles/210413717.
- Account closure page: help.venmo.com/hc/en-us/articles/217532277-Close-Your-Venmo-Account.
- Venmo form to opt out of binding arbitration requirements: help.venmo.com/hc/en-us/articles/360062640153.
- Venmo data science jobs: paypal.eightfold.ai/careers?Job Category=Data Science&Brand=venmo&domain=paypal.com&triggerGoButton=false.

Apps

- Google Play: play.google.com/store/apps/details?id=com.venmo (updated August 24, 2022).
- App Store: apps.apple.com/us/app/venmo/id351727428 (version 9.28.0; August 23, 2022).

Warren, E., "Facilitating Fraud: How Customers Defrauded on Zelle are Left High and Dry by the Banks that Created It," Office of Sen. Elizabeth Warren, Washington, D.C. (October 2022).

Windh, J., "Peer-to-peer payments: Surveying a rapidly changing landscape," Federal Reserve Bank of Atlanta: (August 15, 2011).

Zelle (2022). Legal Terms and Relevant Other Documents:

Legal Terms

- E-sign disclosure and consent: www.zellepay.com/legal/e-sign-disclosure-and-consent (undated).
- User service agreement: www.zellepay.com/legal/user-service-agreement (September 17, 2021).
- Zelle app privacy notice: www.zellepay.com/legal/legal-and-privacy (April 22, 2022).
- Cookies and tracking: www.zellepay.com/legal/cookies-and-tracking-technology (January 3, 2022).
- Terms of use: www.zellepay.com/legal/terms-use (undated).
- "Just in time" notice: www.zellepay.com/legal/just-time-notice (undated form; contains important information about data elements collected via the app).
- Subpoena processing: www.zellepay.com/legal/subpoena-processing (undated).

Other Relevant Documents

- Security page: www.zellepay.com/security.
- How it works: www.zellepay.com/how-it-works (an overview page describing the service).
- Zelle Learning Hub: www.zellepay.com/financial-education/financial-education (general financial literacy resources; not evaluated for quality).

- FAQ page describing how Zelle app can be used only via a smartphone: www.zellepay.com/faq/can-i-access-zelle-send-or-receive-money-without-smartphone.
- Safety page: www.zellepay.com/zelle-safety (does not appear to be linked from Zelle main site nav; discovered via search).
- Contact page: www.zellepay.com/support/contact-support (discovered via search, also linked in footer navigation).

Apps

- Google Play: play.google.com/store/apps/details?id=com.zellepay.zelle&gl=US (updated August 11, 2022).
- App Store: apps.apple.com/us/app/zelle/id1260755201 (version 7.2.0; updated August 11, 2022).