

Rule 1.15: Safekeeping Property

Share:



Client-Lawyer Relationship

(a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated, or elsewhere with the consent of the client or third person. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of [five years] after termination of the representation.

(b) A lawyer may deposit the lawyer's own funds in a client trust account for the sole purpose of paying bank service charges on that account, but only in an amount necessary for that purpose.

(c) A lawyer shall deposit into a client trust account legal fees and expenses that have been paid in advance, to be withdrawn by the lawyer only as fees are earned or expenses incurred.

(d) Upon receiving funds or other property in which a client or third person has an interest, a lawyer shall promptly notify the client or third person. Except as stated in this rule or otherwise permitted by law or by agreement with the client, a lawyer shall promptly deliver to the client or third person any funds or other property that the client or third person is entitled to receive and, upon request by the client or third person, shall promptly render a full accounting regarding such property.

(e) When in the course of representation a lawyer is in possession of property in which two or more persons (one of whom may be the lawyer) claim interests, the property shall be kept separate by the lawyer until the dispute is resolved. The lawyer shall promptly distribute all portions of the property as to which the interests are not in dispute.

ABA American Bar Association |

/content/aba-cms-dotorg/en/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_15_safekeeping_property

Dishonored/Overdraft Check Reporting Rule

Banks in New York State which offer fiduciary accounts to attorneys are required to report all instances of bounced checks and overdrafts on attorney trust, special and escrow accounts. The reports are forwarded to the New York Lawyers' Fund for Client Protection, which serves as a statewide clearing house for these reports. Banks have 10 days to withdraw reports that have been issued in error. If not withdrawn, the reports are sent to the appropriate Attorney Grievance Committee for investigation. A bounced-check and overdraft report generally triggers an audit of the attorney's trust, special or escrow account. The Appellate Divisions' uniform court rule is reported at 22 NYCRR Part 1300.1.

Dishonored Check and Overdraft Reporting Rules for Attorney Special, Trust and Escrow Accounts (22 NYCRR 1300.1):

(a) Special bank accounts required by Disciplinary Rule 9-102 (22 NYCRR 1200.46) shall be maintained only in banking institutions which have agreed to provide dishonored check and overdraft reports in accordance with the provisions of this section.

(b) An agreement to provide dishonored check and overdraft reports shall be filed with the Lawyers' Fund for Client Protection, which shall maintain a central registry of all banking institutions which have been approved in accordance with this section, and the current status of each such agreement. The agreement shall apply to all branches of each banking institution that provides special bank accounts for attorneys engaged in the practice of law in this State, and shall not be cancelled by a banking institution except on 30 days' prior written notice to the Lawyers' Fund for Client Protection.

(c) A dishonored check and overdraft report by a banking institution shall be required whenever a properly payable instrument is presented against an attorney special, trust or escrow account which contains insufficient available funds, irrespective of whether the instrument is honored. A properly payable instrument means an instrument which, if presented in the normal course of business, is in a form requiring payment under the laws of the State of New York.

(d) A dishonored check and overdraft report shall be substantially in the form of the notice of dishonor which the banking institution customarily forwards to its customer, and may include a

photocopy or a computer generated duplicate of such notice.

(e) Dishonored check and overdraft reports shall be mailed to the Lawyers' Fund for Client Protection, 119 Washington Avenue, Albany, NY 12210, within five banking days after the date of presentment against insufficient available funds.

(f) The Lawyers' Fund for Client Protection shall hold each dishonored check and overdraft report for 10 business days to enable the banking institution to withdraw a report provided by inadvertence or mistake; except that the curing of an insufficiency of available funds by a lawyer or law firm by the deposit of additional funds shall not constitute reason for withdrawing a dishonored check and overdraft report.

(g) After holding the dishonored check and overdraft report for 10 business days, the Lawyers' Fund for Client Protection shall forward it to the attorney disciplinary committee for the judicial department or district having jurisdiction over the account holder, as indicated by the law office or other address on the report, for such inquiry and action that attorney disciplinary committee deems appropriate.

(h) Every lawyer admitted to the Bar of the State of New York shall be deemed to have consented to the dishonored check and overdraft reporting requirements of this section. Lawyers and law firms shall promptly notify their banking institutions of existing or new attorney special, trust, or escrow accounts for the purpose of facilitating the implementation and administration of the provisions of this section.

Consumer advisory: Your money is at greater risk when you hold it in a payment app, instead of moving it to an account with deposit insurance

JUN 01, 2023

More than three quarters of adults in the United States have used a payment app [🔗](https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/) (https://www.pewresearch.org/short-reads/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/), sometimes called a P2P (peer-to-peer or person-to-person) app. Widely used nonbank payment apps include PayPal, Venmo, and Cash App. The apps can be used on a computer or mobile device to send money to someone else without writing a check or handing over cash.

Young adults use payment apps even more frequently. According to a [March 2022 survey by Consumer Reports](https://advocacy.consumerreports.org/research/peer-to-peer-payment-services-findings-from-crs-nationally-representative-american-experiences-survey-in-2022/) [🔗](https://advocacy.consumerreports.org/research/peer-to-peer-payment-services-findings-from-crs-nationally-representative-american-experiences-survey-in-2022/) (https://advocacy.consumerreports.org/research/peer-to-peer-payment-services-findings-from-crs-nationally-representative-american-experiences-survey-in-2022/), 85 percent of consumers aged 18 to 29 have used one of these apps.

Money stored in nonbank payment apps often is not protected by federal deposit insurance

Nonbank payment apps help you move money into and out of a linked bank account, credit union account, or card account. They also let you store money inside the app. In fact, money you receive generally stays in your payment app account until you connect to the app and move the money to your linked account.

Keeping money inside your nonbank payment app might feel the same as a keeping money in a traditional bank account with deposit insurance. You can check your balance and review transactions, just as you might do with online banking. However, the difference is that the money in your app might not be held in an account at an FDIC member bank or NCUA member credit union.

This means it might not offer federal deposit insurance.

The difference is key because money you keep in your bank or credit union account is insured if the bank or credit union fails. However, deposit insurance does not apply when a nonbank payment company fails. When you consider the worst-case scenario, you might wonder: What if the payment company holding my money goes out of business or fails?

If a payment app's business fails, what happens next is often unclear

Apps can be set up in different ways, with different business models, investment strategies, and risks. Your payment app company might invest your money in loans and bonds, instead of keeping the money in a bank or credit union account. The company can earn money on these investments, while generally paying no interest to you. The payment app's business could be at risk from investment losses, interest rate changes, currency exchange rates, and liquidity problems.

Your user agreement might be confusing, murky, or even silent on exactly where your money is held or invested. It might not explain whether and under what conditions your money may be insured at a bank or credit union, and what happens in the case of the nonbank payment app's business failure or bankruptcy.

In contrast, money you deposit in an account at an insured bank or credit union is protected up to the insurance limit if the firm fails. The Federal Deposit Insurance Corporation (FDIC) and National Credit Union Administration (NCUA) protect deposits up to \$250,000 under the same owner or owners. If your bank or credit union fails, you still have quick access to your money.

If the nonbank payment app's business fails, your money is likely lost or tied up in a long bankruptcy process. You might be standing in line with other lenders to the failed app, waiting to see if you can get any of your money back after the business is unwound.

Some apps offer "pass-through" insurance, if you take additional steps

Some apps may claim to provide pass-through insurance through business arrangements with a bank or credit union for customers who sign up for additional services. For example, you might have to get a company-branded card or choose direct deposit. To be eligible for pass-through insurance, the account must comply with certain rules and regulations set by the FDIC or

NCUA.

Pass-through insurance means you are insured against the failure of the bank or credit union where the app holds the money for you. It doesn't insure you against the failure of the payment app company. This means there could be a risk of losing your money in the event the company fails. If the payment app company followed all the relevant requirements, though, your money could be safe in the associated bank or credit union. Still, there could be risks, like delaying your ability to access your money.

Tip: Send yourself a reminder to move your money from the app to your insured account

Planning on moving your balance from your payment app into your linked account? Use [this link](#) to send yourself an e-mail reminder - or share it with a friend or family member.

What the CFPB is doing

We're taking steps to help you spot the risks and help with problems related to leaving money in a payment app:

- [Issue Spotlight](http://cfpb.gov/data-research/research-reports/issue-spotlight-analysis-of-deposit-insurance-coverage-on-funds-stored-through-payment-apps/) (cfpb.gov/data-research/research-reports/issue-spotlight-analysis-of-deposit-insurance-coverage-on-funds-stored-through-payment-apps/) - See a summary of popular payment apps and how your funds might or might not be protected
- [Ask CFPB](#) () - Get clear, impartial answers to common money questions, including [Is the money I keep in my payment app safe?](http://cfpb.gov/askcfpb/2135) (cfpb.gov/askcfpb/2135)
- [Submit a complaint to the CFPB](http://www.consumerfinance.gov/complaint) (http://www.consumerfinance.gov/complaint) if you have a problem with a financial product or service, including problems with moving money out of an app

PRESS INFORMATION

If you want to republish the article or have questions about the content, please contact the press office.

FURTHER READING

 **Blog**

What's ahead for Bank of America and its customers (cfpb.gov/about-us/blog/whats-ahead-for-bank-of-america-and-its-customers/)

JUL 19, 2023

Qué viene a continuación para Bank of America y sus clientes (cfpb.gov/about-us/blog/que-viene-a-continuacion-para-bank-of-america-y-sus-clientes/)

JUL 19, 2023

Sa ki rezève pou Bank of America ak kliyan li yo (cfpb.gov/about-us/blog/whats-ahead-for-bank-of-america-and-its-customers-ht/)

JUL 19, 2023

[View more](https://cfpb.gov/activity-log/?topics=electronic-payments&topics=banking) (cfpb.gov/activity-log/?topics=electronic-payments&topics=banking)



PRESS RELEASE

Consumer Reports finds peer-to-peer payment apps offer ease and convenience but pose potential financial and privacy risks for users

January 24, 2023

CR identifies steps that providers can take to improve protections and offers tips to consumers for reducing risks

YONKERS, NY – A new [Consumer Reports evaluation](http://consumerreports.org/money/digital-payments/peer-to-peer-payment-apps-comparison-a5999129619/) of popular peer-to-peer (P2P) payment apps found that users could lose money to fraud or scams and face privacy risks because app providers may share their personal information widely and it is difficult for users to delete their data. CR is calling on P2P payment providers to strengthen their consumer disclosures and app features and is offering tips to users to help avoid problems.

"Peer-to-peer payment apps are a convenient and easy way to send money to others with just a few taps on your phone," said Delicia Hand, director of financial fairness for Consumer Reports. "But consumers may end up losing money if they send a payment to the wrong person or fall victim to fraud or scams and are putting their privacy at risk when using a P2P payment app."

Consumer Reports evaluated P2P payment apps (<https://advocacy.consumerreports.org/research/peer-to-peer-payment-apps-a-case-study-for-a-digital-finance-standard/>) using its [Fair Digital Finance Framework](https://advocacy.consumerreports.org/issue/money/financial-fairness/), which CR developed to examine the benefits of digital finance products and services and the potential risks they may pose for consumers. The Framework was created with input from academics, fintech companies, regulators and consumer advocates to identify consumer friendly practices, improve industry practices and spur policymakers to adopt needed safeguards.

Recent surveys by Consumer Reports (<https://advocacy.consumerreports.org/research/peer-to-peer-payment-services-findings-from-crs-nationally-representative-american-experiences-survey-in-2022/>) have documented how widely P2P payment services are used in the U.S. Well over half of Americans (64 percent) use a P2P payment app for payments to and from individuals, including four out of five (81 percent) of the 18 to 29 age group, according to a March 2022 nationally representative CR survey of 2,116 U.S. adults. Two out of five Americans (40 percent) say they use P2P payment services at least once a month; nearly one in five (18 percent) use them at least once a week.

While P2P payment apps have proven popular, users can lose money when they accidentally make an

erroneous payment or fall victim to fraud or scams. CR's survey found that of those who use P2P payment services at least once per week, 12 percent had sent money to the wrong person and 9 percent had been the victim of a scam.

In August through October 2022, CR examined Apple Cash, Cash App, Venmo and Zelle, and focused on the app providers' safety, privacy and transparency policies, practices and protections by examining publicly available documents found on company websites and apps. CR evaluated safety practices related to the technology and policies used by the companies to protect consumer data and funds; privacy practices related to user data collection, sharing, and deletion; and transparency practices related to company disclosures of legal terms and consumer rights. Consumer disclosures were often difficult to find and understand, raising broad concerns about transparency. CR found that:

- All four P2P payment apps do not fully reimburse customers when users are induced into fraud. Although Venmo says that it will fully compensate users in these cases, and even has a purchase protection program for certain qualifying purchases, payments authorized by the user that exceed the initial authorization are not covered unless the user notifies Venmo and rescinds the authorization. None of the four apps will reimburse users or otherwise intervene when a payment is accidentally sent to the wrong person.
- All four P2P payment apps collect a large amount of personally identifying information about their users, may share it with undisclosed companies for sometimes unknown or vague purposes, and make it difficult for users to delete their own data. The P2P payment apps appear to collect far more data, and more types of data, than they need to provide the services that consumers expect.
- Apple Cash, Cash App, and Venmo have to meet sometimes confusing conditions to ensure their funds held in the payments portion of the app are protected by Federal Deposit Insurance Corporation insurance. Users could lose money if they haven't completed additional app or product registration requirements and the P2P companies suffer financial losses or declare bankruptcy.
- All four P2P payment apps make it very difficult for users to track changes to the legally binding terms governing the service and require users to give up certain legal rights to resolve disputes. Users must resolve claims and disputes on an individual basis, mostly through binding arbitration or small claims court.

CR has urged policymakers to strengthen consumer protections for P2P payment app users, but is calling on providers not to wait for regulators to act. "P2P payment providers can raise the bar for consumer protection by taking more aggressive steps to minimize user risks," said Hand. "Adopting stronger policies and safeguards will help build customer trust and loyalty and establish a new industry standard for fair digital finance." CR recommends that providers:

- Clearly state which security protocols are used to protect users' information.
- Be transparent about the availability of FDIC insurance and clearly explain reimbursement policies in cases of fraud or error.
- Go beyond obligations to investigate and resolve only certain fraud and scams under Regulation E of the Electronic Funds Transfer Act. For example, providers could create a fund to reimburse users who are victims of scams and tricked into transferring money.
- Collect only the data needed to prevent fraud and provide the payment service. Disclose and

identify, in consumer-facing, legally binding terms and conditions, the data collected, 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 provide the service
- Do not require users to agree to binding arbitration to resolve disputes or to resolve claims on an individual basis

CR recommends a number of steps consumers can take to help minimize potential risks:

- **Confirm the recipient's identity before sending money.** Do that with a phone number, email address, or a QR code. Cash App, Venmo and Zelle give users the ability to scan a QR code that appears on the recipient's device.
- **Send a \$1 test payment and confirm it was received by the right person.** That's especially important if you are sending a lot of money.
- **Move money from your P2P account to your bank account as soon as possible.** That assures your funds are FDIC insured in your bank.
- **Turn on all identity verification options available in the P2P app.** With those features activated, anyone trying to use the account will have to go through additional security measures, such as two-factor authentication.
- **Frequently monitor your P2P accounts.** You may be able to catch problems early enough to report it to companies and not be on the hook for unauthorized payments.
- **Delete any P2P app you don't use.** It's not enough to simply remove the app from your phone; instead, to make sure you've closed and deleted the account, select the "delete account" option within the app.
- **Opt out of binding arbitration if possible.** Cash App, Venmo and Zelle give users 30 days to opt out of the requirement by mailing a written notice. Apple Cash does not allow users to opt out. And if you do have a dispute, try negotiating with the company before going to arbitration.

Consumer Reports' assessment of peer-to-peer payment apps is part of a broader initiative to strengthen consumer protections in the burgeoning digital finance marketplace, made possible, in part, by a grant from Flourish Ventures' fund at the Silicon Valley Community Foundation. The grant supports CR's efforts to partner with consumers, industry, and policymakers to secure business practices, standards, and laws necessary to build a fair and inclusive financial marketplace.

Michael McCauley, michael.mccauley@consumer.org, 415-902-9537

Delicia Hand

Director, Financial Fairness Advocacy

You Might Also Be Interested In

August 17, 2023

Consumer Reports memo of support for New York bills that strengthen protections for private student loan borrowers
(<http://advocacy.consumerreports.org/research/consumer-reports-memo-of-support-for-new-york-bills-that-strengthen-protections-for-private-student-loan-borrowers/>)

August 17, 2023

CR memo of support for New York's proposed Consumer and Small Business Protection Act
(<http://advocacy.consumerreports.org/research/cr-memo-in-support-of-new-yorks-proposed-consumer-and-small-business-protection-act/>)

PRESS RELEASE

August 16, 2023

Consumer Reports praises CFPB for its plans to rein in abusive data broker practices
(http://advocacy.consumerreports.org/press_release/consumer-reports-praises-cfpb-for-its-plans-to-rein-in-abusive-data-broker-practices/)

August 16, 2023

Consumer Reports letter to the CFPB on data broker abuses
(<http://advocacy.consumerreports.org/research/consumer-reports-letter-to-the-cfpb-on-data-broker-abuses/>)



(<https://www.consumerreports.org/>)

Member Support

Contact Us (<https://www.consumerreports.org/member-support/>)

Account Settings (<https://secure.consumerreports.org/ec/account/overview>)

What is Membership? (<https://www.consumerreports.org/membership/>)

Make a Donation (https://donate.consumerreports.org/donation/15?processing_fee_enabled=true&INTKEY=3021000245&one_time_ask=1000%7C500%7C100%7C50%7C35&one_time_ask_selected=4&monthly_ask=104%7C52%7C10%7C7%7C5&monthly_ask_selected=2)

Newsletters (<https://www.consumerreports.org/email-newsletters?INTKEY=I970GB1N&source=I970GB1N>)

Give a Gift (<https://www.consumerreports.org/gift/>)

About

About Us (<https://www.consumerreports.org/cro/about-us/what-we-do/index.htm>)

Career Opportunities (<https://www.consumerreports.org/cro/careers/landing-page/index.htm>)

Media Room (<https://www.consumerreports.org/media-room/>)

Advocacy (<https://advocacy.consumerreports.org/>)

CR Recommended Program (<https://www.consumerreports.org/cr-recommended/>)

Data Intelligence (<https://data.consumerreports.org/>)

Innovation (<https://innovation.consumerreports.org/>)

Product Reviews

Appliances (<https://www.consumerreports.org/appliances/>)

Babies & Kids (<https://www.consumerreports.org/babies-kids/>)

Cars (<https://www.consumerreports.org/cars/>)

Electronics (<https://www.consumerreports.org/electronics-computers/>)

Health (<https://www.consumerreports.org/health/>)

Home & Garden (<https://www.consumerreports.org/home-garden/>)

Money (<https://www.consumerreports.org/money/>)

A-Z Index (<https://www.consumerreports.org/cro/a-to-z-index/products/index.htm>)

Magazine & Books

Current Issue (<https://www.consumerreports.org/magazine/2023/09/>)

CR Magazine Archive (<https://www.consumerreports.org/magazine/2023/>)

5 Year Index (<https://article.images.consumerreports.org/prod/content/dam/cro/corporate/customer-service/5-year-index.pdf>)

CR Store (<https://www.consumerreports.org/cr-store/>)



American Experiences Survey:
A Nationally Representative Multi-Mode Survey
March 2022 Omnibus Results

Overview of Methodology

Each month, Consumer Reports fields the American Experiences Survey (AES) to track consumer attitudes and behaviors over time. March results are based on interviews conducted from March 11-22, 2022. This document includes all sections of the omnibus survey for this month: COVID-19, peer-to-peer payment services, auto buying priorities, second opinions on dental work, and brainpower (memory/cognitive function).

The survey was administered by NORC at the University of Chicago through its AmeriSpeak® Panel to a nationally representative sample. Interviews were conducted in English and in Spanish, and were administered both online and by phone. In total NORC collected 2,116 interviews, 1,982 by web mode and 134 by phone mode, 2,031 in English and 85 in Spanish. Final data are weighted by age, gender, race/Hispanic ethnicity, housing tenure, telephone status, education, and Census Division to be proportionally representative of the US adult population.

The margin of error for results based on the total sample is +/-2.83 percentage points at the 95% confidence level. Smaller subgroups will have larger error margins, and only those subgroups for which there are at least 100 unweighted cases are included.

TOPLINE RESULTS WITH MONTHLY TRENDS

The March omnibus contained five blocks of questions (items on COVID-19, peer-to-peer payment services, auto buying priorities, dental second opinions, and brainpower). Respondents saw the COVID-19 block first and the brainpower block last, with the other three sections in a randomized order in between.

The questions presented below were shown to respondents in this order unless otherwise noted. Where appropriate, question verbiage, response answer choices, or direction of scales were randomized or rotated and those instances are noted below.

Also shown, where available, are trends over time. Not every item was asked on every recent omnibus survey, and where minor revisions to the wording of an item or response choices were made, they are noted below. *Note these changes may impact comparability of results.*

Prepared by CR Survey Research Department, April 2022

www.cr.org

Survey Notes for Monthly Trends

March 2022 results are based on interviews conducted from March 11-22 with a nationally representative sample of 2,116 US adults.

February 2022 results are based on interviews conducted from February 14-22 with a nationally representative sample of 2,640 US adults.

January 2022 results are based on interviews conducted from January 7-20 with a nationally representative sample of 2,174 US adults.

December 2021 results are based on interviews conducted from December 13-22 with a nationally representative sample of 2,073 US adults.

November 2021 results are based on interviews conducted from November 5-15 with a nationally representative sample of 2,057 US adults.

October 2021 results are based on interviews conducted from October 12-21 with a nationally representative sample of 2,036 US adults.

September 2021 results are based on interviews conducted from September 13-22 with a nationally representative sample of 2,341 US adults.

August 2021 results are based on interviews conducted from August 6-17 with a nationally representative sample of 2,165 US adults.

July 2021 results are based on interviews conducted from July 12-21 with a nationally representative sample of 2,184 US adults.

June 2021 results are based on interviews conducted from June 11-22 with a nationally representative sample of 2,280 US adults.

May 2021 results are based on interviews conducted from May 7-17 with a nationally representative sample of 2,079 US adults.

April 2021 results are based on interviews conducted from April 9-19 with a nationally representative sample of 2,288 US adults.

March 2021 results are based on interviews conducted from March 4-15 with a nationally representative sample of 2,144 US adults.

February 2021 results are based on interviews conducted from February 4-15 with a nationally representative sample of 2,514 US adults.

January 2021 results are based on interviews conducted from January 7-19 with a nationally representative sample of 2,233 US adults.

December 2020 results are based on interviews conducted from December 10-21 with a nationally representative sample of 2,982 US adults.

November 2020 results are based on interviews conducted from November 5-16 with a nationally representative sample of 2,851 US adults.

October 2020 results are based on interviews conducted from October 8-26 with a nationally representative sample of 2,670 US adults.

September 2020 results are based on interviews conducted from September 11-21 with a nationally representative sample of 2,303 US adults.

August 2020 results are based on interviews conducted from August 7-19 with a nationally representative sample of 2,236 US adults.

Survey Notes for Monthly Trends, cont'd.

July 2020 results are based on interviews conducted from July 9-20 with a nationally representative sample of 2,031 US adults.

June 2020 results are based on interviews conducted from June 4-16 with a nationally representative sample of 1,014 US adults.

May 2020 results are based on interviews conducted from May 8-18 with a nationally representative sample of 2,085 US adults.

COVID-19

COVCONCERNNOW.

How concerned or not concerned are you about COVID-19 continuing to spread in your local area over the next month?

	MARCH 2022 AES	FEBRUARY 2022 AES	JANUARY 2022 AES	DECEMBER 2021 AES	NOVEMBER 2021 AES	OCTOBER 2021 AES	SEPTEMBER 2021 AES
	Total	Total	Total	Total	Total	Total	Total
	%	%	%	%	%	%	%
Very concerned	18	23	45	37	24	26	41
Somewhat concerned	32	35	33	32	38	41	35
Not too concerned	34	28	15	19	26	24	16
Not concerned at all	16	15	8	11	11	9	9
Base: All respondents	2,109	2,636	2,171	2,069	2,054	2,032	2,338

(continued)

	AUGUST 2021 AES	JULY 2021 AES	JUNE 2021 AES	MAY 2021 AES	APRIL 2021 AES	MARCH 2021 AES	FEBRUARY 2021 AES
	Total	Total	Total	Total	Total	Total	Total
	%	%	%	%	%	%	%
Very concerned	40	25	14	19	28	30	40
Somewhat concerned	36	34	35	34	38	34	36
Not too concerned	15	25	33	33	22	25	17
Not concerned at all	9	16	17	15	12	11	7
Base: All respondents	2,164	2,178	2,278	2,078	2,287	2,140	2,514

(continued)

	DECEMBER 2020 AES	NOVEMBER 2020 AES	OCTOBER 2020 AES	SEPTEMBER 2020 AES	AUGUST 2020 AES	JULY 2020 AES	JUNE 2020 AES	MAY 2020 AES
	Total	Total	Total	Total	Total	Total	Total	Total
	%	%	%	%	%	%	%	%
Very concerned	51	51	44	42	44	53	41	41
Somewhat concerned	30	30	32	33	34	29	34	36
Not too concerned	13	14	17	18	16	12	16	18
Not concerned at all	6	5	6	7	6	5	8	6
Base: All respondents	2,977	2,850	2,668	2,300	2,233	2,031	1,014	2,082

COVCONCERN6MOS.

How concerned or not concerned are you about COVID-19 continuing to spread in your local area over the next 6 months?

	MARCH 2022 AES	FEBRUARY 2022 AES	JANUARY 2022 AES	DECEMBER 2021 AES	NOVEMBER 2021 AES	OCTOBER 2021 AES
	Total	Total	Total	Total	Total	Total
	%	%	%	%	%	%
Very concerned	17	22	39	36	25	24
Somewhat concerned	34	35	36	33	37	43
Not too concerned	32	28	17	20	27	24
Not concerned at all	17	15	8	11	11	10
Base: All respondents	2,084	2,611	2,143	2,041	2,032	2,003

(continued)

	SEPTEMBER 2021 AES	AUGUST 2021 AES	JULY 2021 AES	JUNE 2021 AES	MAY 2021 AES	APRIL 2021 AES	MARCH 2021 AES
	Total	Total	Total	Total	Total	Total	Total
	%	%	%	%	%	%	%
Very concerned	39	38	25	15	17	26	26
Somewhat concerned	36	37	34	34	35	37	36
Not too concerned	17	16	24	34	32	25	27
Not concerned at all	8	10	17	17	16	12	12
Base: All respondents	2,311	2,144	2,162	2,251	2,055	2,275	2,123

	FEBRUARY 2021 AES	DECEMBER 2020 AES	NOVEMBER 2020 AES	OCTOBER 2020 AES	SEPTEMBER 2020 AES	AUGUST 2020 AES	JULY 2020 AES
	Total	Total	Total	Total	Total	Total	Total
	%	%	%	%	%	%	%
Very concerned	35	44	49	45	41	44	53
Somewhat concerned	38	34	32	31	35	33	29
Not too concerned	20	15	14	18	17	17	13
Not concerned at all	8	6	6	7	7	6	6
Base: All respondents	2,505	2,948	2,809	2,643	2,282	2,214	2,031

COVCHILDAGE. [‘I DO NOT HAVE ANY CHILDREN’ IS EXCLUSIVE.]

Do you currently have any children living in your household who are...?	
Select <u>all</u> that apply.	
	Total
	%
Under 2 years old	6
2 to 4 years old	10
5 to 11 years old	19
12 to 15 years old	11
16 to 17 years old	8
I do not have any children under 18 years old living in my household	63
Base: All respondents	2,116

COVCHILDVAC_INTRO. [SHOW IF COVCHILDAGE = ‘UNDER 2 YEARS OLD’ OR ‘2 TO 4 YEARS OLD.’]

As of the fielding of this survey, COVID-19 vaccines have been approved for use in children aged 5 and up. Vaccines for younger children are expected to be authorized over the coming months.

COVCHILDVAC2. [SHOW IF COVCHILDAGE = ‘UNDER 2 YEARS OLD’ OR ‘2 TO 4 YEARS OLD.’ SHOW EACH AGE GROUP TO RESPONDENTS WHO HAVE CHILDREN IN THAT AGE GROUP IN THE HOUSEHOLD.]

Thinking about your child (or children) in each of the age groups below, what is the likelihood that you will have them get a COVID-19 vaccine <u>if/when one becomes available</u> to children their age?						
	MARCH 2022 AES	FEBRUARY 2022 AES	DECEMBER 2021 AES	NOVEMBER 2021 AES	JUNE 2021 AES	MAY 2021 AES
	Total	Total	Total	Total	Total	Total
	%	%	%	%	%	%
Under 2 years old						
Very likely	26	30	27	20	18	16
Somewhat likely	15	18	13	25	22	26
Not too likely	10	21	13	12	15	17
Not at all likely	49	32	47	43	45	42
Base: Respondents with children under 2 years old living in the household	121	156	108	148	142	130
2 to 4 years old						
Very likely	24	26	20	19	15	16
Somewhat likely	15	16	20	24	28	25
Not too likely	18	15	19	14	22	13
Not at all likely	43	43	41	43	35	45
Base: Respondents with children 2 to 4 years old living in the household	186	197	150	215	259	224

Note: Prior to November 2021, age categories included 2 to 5 years old and 6 to 11 years old.

PEER-TO-PEER PAYMENT SERVICES

P2P_INTRO.

This section asks about peer-to-peer payment services, also called money transfer apps, such as PayPal, Venmo, Apple Pay, Google Pay, or Zelle. These services allow users to send and receive money to one another directly through their smartphones, tables, or computers without using cash or checks.

Some of these services can also be used to pay in stores or online. However, in this section, *we are only interested in person-to-person payments, not payments to businesses. We are interested in payments for services, such as for babysitting or home repair.*

P2P1. [REQUEST RESPONSE IF LEFT UNANSWERED.]

How often, if ever, do you use peer-to-peer payment services?

Remember to answer only for payments you make to or receive from other people, not payments you make through one of these services when purchasing something at a store or online.

	Total
	%
Daily	5
At least once a week, but less than daily	13
At least once a month, but less than weekly	23
Less often than once a month	23
I used to use this kind of service, but do not now	5
I have never used peer-to-peer payment services	31
Base: All respondents	2,114

P2P2. [SHOW IF P2P1 = 'DAILY,' 'AT LEAST ONCE A WEEK,' OR 'AT LEAST ONCE A MONTH.' RESPONSE OPTIONS DISPLAYED IN ALPHABETICAL ORDER, WITH 'OTHER' HELD AT END.]

You said that you use peer-to-peer payment systems for payments to or from other people at least sometimes. Which peer-to-peer payment services do you currently use regularly for payments to or from other people?

By "regularly," we mean services that you have active accounts with and use at least once a month. Again, please answer only for payments you make to or receive from other people, not for purchases made in stores or online.

Select all that apply.

	Total
	%
PayPal	49
Venmo	48
Cash App	40
Zelle	39
Apple Pay Cash	19
Google Pay	10
Facebook Pay	9
Western Union	4
Remitly	0
Other, please specify	3
Base: Respondents who use peer-to-peer payment systems at least once a month	847

P2P3. [SHOW IF P2P1 = 'DAILY,' 'AT LEAST ONCE A WEEK,' 'AT LEAST ONCE A MONTH,' 'LESS OFTEN THAN ONCE A MONTH,' OR 'USED TO USE THIS KIND OF SERVICE, BUT DO NOT NOW.' QUESTION STEM AND RESPONSE OPTIONS HAD SLIGHTLY DIFFERENT WORDING FOR CURRENT USERS THAN FOR RESPONDENTS WHO SAID 'USED TO USE THIS KIND OF SERVICE,' AS SHOWN BELOW. RESPONSE OPTIONS DISPLAYED IN THIS ORDER: CHECKING ACCOUNT; DEBIT CARD; CREDIT CARD; PREPAID CARD; BALANCE IN THE ACCOUNT FROM MONEY RECEIVED; CRYPTOCURRENCY WALLET; OTHER.]

[If respondent said they use a peer-to-peer service "less often than once a month" or more frequently:] You said that you currently use at least one peer-to-peer payment service. Typically when someone uses this type of account, the money that is transferred comes from a checking account, prepaid card, or balance in the account; is charged to a credit card; or comes from a cryptocurrency wallet linked to the account. Which of the following is most common for you?

[If respondent said they "used to use this kind of service, but do not now:]" You said that you used to use at least one peer-to-peer payment service. Typically when someone uses this type of account, the money that is transferred comes from a checking account, prepaid card, or balance in the account; is charged to a credit card; or comes from a cryptocurrency wallet linked to the account. Which of the following was most common for you?

If you [have/had] more than one peer-to-peer payment service, please answer for the one you [use/used] most.

Not all of these options are possible with every peer-to-peer service.

	Total
	%
The money [is / was] withdrawn straight from my checking account to my P2P account	51
The money [is / was] withdrawn from my checking account through a debit card that [is/was] linked with my P2P account	26
Payments I [make / made] through this service [are / were] charged to a credit card that [is/was] linked with my P2P account	9
The money [is / was] withdrawn from a balance I [keep / kept] in the P2P account from money other people [have/had] sent me	6
The money [is / was] withdrawn from a prepaid card that [is / was] linked to my P2P account	4
The money [comes / came] from a cryptocurrency wallet linked to this P2P account	1
Other, please specify	3
Base: Respondents who have ever used a peer-to-peer payment service	1,464

P2P4. [SHOW IF P2P1 = 'DAILY,' 'AT LEAST ONCE A WEEK,' 'AT LEAST ONCE A MONTH,' 'LESS OFTEN THAN ONCE A MONTH,' OR 'USED TO USE THIS KIND OF SERVICE, BUT DO NOT NOW.' QUESTION STEM HAD SLIGHTLY DIFFERENT WORDING FOR CURRENT USERS THAN FOR RESPONDENTS WHO SAID 'USED TO USE THIS KIND OF SERVICE,' AS SHOWN BELOW. RANDOMIZE RESPONSE OPTIONS, HOLDING 'OTHER' AND 'NEVER HAD ANY ISSUES' AT END IN THAT ORDER.]

[If respondent said they use a peer-to-peer service "less often than once a month" or more frequently:] You said that you currently use at least one peer-to-peer payment service. Which, if any, of the following issues have you had sending or receiving money through a peer-to-peer payment service?

[If respondent said they "used to use this kind of service, but do not now:"] You said that you used to use at least one peer-to-peer payment service. Which, if any, of the following issues did you have sending or receiving money through a peer-to-peer payment service?

Note that these can be technical issues or other problems.

Select all that apply.

	Total
	%
Sending money to the wrong person	6
Sending money for what turned out to be a scam	6
Sending money to someone that was never received	6
Not receiving money that was sent to you	4
Receiving money from someone you don't know (sent to you mistakenly)	3
Other, please specify	2
You have never had any issues with a peer-to-peer payment service	78
Base: Respondents who have ever used a peer-to-peer payment service	1,483

P2P5. [SHOW IF ANY ISSUES WERE SELECTED IN P2P4 (INCLUDING 'OTHER'). RANDOMIZE RESPONSE OPTIONS, HOLDING 'OTHER' AND 'DID NOT TRY TO RESOLVE THE ISSUES' AT END IN THAT ORDER.]

You said that you have had at least one issue with a peer-to-peer payment service. Which, if any, of the following did you do to try to resolve the issue(s)?

Select all that apply.

	Total
	%
Contacted the service provider (e.g., Venmo or Zelle)	48
Contacted the person who received the money from me	41
Contacted the person who sent the money to me	27
Other, please specify	5
I did not try to resolve the issue(s)	9
Base: Respondents who had at least one issue with a peer-to-peer payment service	294

P2P6. [SHOW IF P2P5 = 'CONTACTED THE SERVICE PROVIDER.' RESPONSE OPTIONS DISPLAYED IN THIS ORDER: DIFFICULT TO LOCATE CONTACT PHONE NUMBER; ON HOLD FOR A LONG TIME; DIFFICULT TO LOCATE CONTACT INFORMATION FOR ONLINE SUPPORT; DIFFICULT TO GET A RESPONSE FROM ONLINE SUPPORT; OTHER; I HAD NO ISSUES.]

You said that you have tried to resolve at least one issue with a peer-to-peer payment service by contacting the service provider. Which, if any, of the following are issues you had accessing assistance from the service provider?

Select all that apply.

	Total
	%
I found it difficult to get a response from online support	39
I found it difficult to locate a contact phone number	36
I was on hold for a long time when I called	35
I found it difficult to locate contact information for online support	30
Other, please specify	5
I had no issues accessing assistance from the service provider	23
Base: Respondents who tried to resolve an issue by contacting the P2P service provider	129

P2P7. [SHOW IF P2P5 = ANY ATTEMPTED RESOLUTION, INCLUDING 'OTHER.' RANDOMIZE RESPONSE OPTIONS, HOLDING 'OTHER' AND 'I WAS NOT ABLE TO RESOLVE THE ISSUE' AT END IN THAT ORDER.]

When you tried to resolve your most recent issue with a peer-to-peer payment service, what was the outcome?

Select all that apply.

	Total
	%
The service provider resolved the issue	26
I was reimbursed by the person who received the money from me	22
I reimbursed the person who mistakenly sent the money to me	15
The person who sent me money had to send it a second time	14
I had to pay the person I sent money to a second time	12
Other, please specify	6
I was not able to resolve the issue	21
Base: Respondents who tried to resolve an issue with a P2P service	265

AUTO BUYING PRIORITIES

CAR1. [REQUEST RESPONSE IF LEFT UNANSWERED.]

Are you considering buying or leasing a new or used car or truck within the next year?	
	Total
	%
Yes	28
No	72
Base: All respondents	2,116

CAR2. [REQUEST RESPONSE TWICE IF LEFT UNANSWERED.]

Do you currently have a valid driver's license?	
	Total
	%
Yes	91
No	9
Base: All respondents	2,115

CAR3. [SHOW IF CAR1 = 'YES.' RESPONSE OPTIONS SHOWN IN THIS ORDER: NEW; USED.]

You said that you are considering buying or leasing a car or truck in the next year. In your decision of what to buy or lease, are you considering...?	
<i>Select <u>all</u> that you are considering.</i>	
	Total
	%
Used	58
New	58
Base: Respondents considering getting a vehicle in the next year	602

CAR4. [RESPONSE OPTIONS DISPLAYED IN ALPHABETICAL ORDER.]

Below are several factors that people may consider when in the market for a car or truck. Please select all factors, if any, that are not important to you at all—that is, that would not affect your decision of which vehicle to purchase or lease in any way.

Select all that apply.

	Total
	%
Off-road capability	40
Brand	38
Towing capability	36
Latest technology	36
Purchase price	35
Fuel economy	33
Reliability	30
Connectivity	29
Safety	29
Horsepower	29
Vehicle size	29
Cargo space	27
Style	26
Vehicle comfort	26
Maintenance cost	26
Passenger space	25
Range (how far you can drive your vehicle on a full tank of gas or full charge)	24
Handling	18
Base: All respondents	2,116

CAR5. [ALL RESPONSE OPTIONS NOT SELECTED IN CAR4 DISPLAYED IN ALPHABETICAL ORDER. RESPONSES LIMITED TO FIVE. ITEM NOT SHOWN TO RESPONDENTS WHO LEFT FIVE OR FEWER CHOICES BLANK IN CAR4; IN THIS CASE, RESPONSES TO CAR5 WERE AUTOMATICALLY SELECTED (EVERYTHING LEFT BLANK IN CAR4).]

Here are all the factors you said would affect your decision of which vehicle to purchase or lease. Which are the most important to you personally when making your decision about which vehicle to purchase or lease?

Select up to five.

	Total
	%
Purchase price	44
Fuel economy	41
Reliability	36
Maintenance cost	34
Safety	32
Vehicle comfort	24
Handling	22
Brand	21
Range (how far you can drive your vehicle on a full tank of gas or full charge)	20
Passenger space	19
Vehicle size	18
Cargo space	16
Style	13
Latest technology	12
Horsepower	12
Connectivity	9
Off-road capability	8
Towing capability	8
Base: All respondents (each respondent only saw items they <u>did not</u> select in CAR4, but percentages are out of full sample)	2,099

CAR6. [EACH RESPONDENT SAW THE FACTORS THEY SELECTED IN CAR5 IN A RANDOMIZED ORDER. IF RESPONDENT GAVE THE SAME RANKING TO MORE THAN ONE RESPONSE OPTION, THE FOLLOWING PROMPT APPEARED: 'YOU HAVE GIVEN THE SAME RANKING TO MORE THAN ONE ITEM. PLEASE GIVE EACH ITEM A UNIQUE RATING.' IF RESPONDENT SKIPPED AN ITEM—SUCH AS IF RESPONDENT ONLY SELECTED FOUR ITEMS AND RANKED THEM 1, 3, 4, 5—THE FOLLOWING PROMPT APPEARED: 'WE NOTICED THAT YOU SKIPPED A NUMBER IN YOUR RANKING. PLEASE REVIEW YOUR ANSWERS TO MAKE SURE THEY ARE CORRECT.' ITEM NOT SHOWN TO RESPONDENTS WHO SELECTED ONLY ONE CHOICE IN CAR5; IN THIS CASE, THAT ITEM WAS AUTOMATICALLY SET AS 'MOST IMPORTANT' IN CAR6.]

These are the factors you said would be most important in your decision of which vehicle to purchase or lease. Please rank them in order from <u>most to least important</u> for you.	
	Total
	%
Brand	
1 Most important	5
2 Second most important	5
3 Third most important	3
4 Fourth most important	3
5 Least important	4
(Not in top five*)	79
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Cargo space	
	Total
1 Most important	2
2 Second most important	3
3 Third most important	4
4 Fourth most important	4
5 Least important	3
(Not in top five*)	85
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Connectivity	
	Total
1 Most important	1
2 Second most important	2
3 Third most important	2
4 Fourth most important	2
5 Least important	1
(Not in top five*)	92
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116

*"Not in top five" is calculated for reporting purposes based on responses to CAR5. It was not offered as a response option.

CAR6. [CONTINUED.]

Fuel Economy	Total
1 Most important	7
2 Second most important	11
3 Third most important	9
4 Fourth most important	9
5 Least important	5
(Not in top five*)	59
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Handling	Total
1 Most important	3
2 Second most important	6
3 Third most important	6
4 Fourth most important	4
5 Least important	4
(Not in top five*)	78
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Horsepower	Total
1 Most important	1
2 Second most important	3
3 Third most important	3
4 Fourth most important	3
5 Least important	2
(Not in top five*)	88
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Latest technology	Total
1 Most important	2
2 Second most important	2
3 Third most important	3
4 Fourth most important	2
5 Least important	3
(Not in top five*)	88
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Maintenance cost	Total
1 Most important	5
2 Second most important	8
3 Third most important	8
4 Fourth most important	6
5 Least important	5
(Not in top five*)	67
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116

***Not in top five" is calculated for reporting purposes based on responses to CAR5. It was not offered as a response option.*

CAR6. [CONTINUED.]

Off-road capability	Total
1 Most important	1
2 Second most important	2
3 Third most important	2
4 Fourth most important	2
5 Least important	2
(Not in top five*)	92
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Passenger space	Total
1 Most important	3
2 Second most important	3
3 Third most important	4
4 Fourth most important	4
5 Least important	5
(Not in top five*)	81
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Purchase price	Total
1 Most important	24
2 Second most important	8
3 Third most important	6
4 Fourth most important	3
5 Least important	3
(Not in top five*)	56
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Range (how far you can drive your vehicle on a full tank of gas or full charge)	Total
1 Most important	6
2 Second most important	4
3 Third most important	4
4 Fourth most important	3
5 Least important	3
(Not in top five*)	80
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Reliability	Total
1 Most important	10
2 Second most important	11
3 Third most important	7
4 Fourth most important	5
5 Least important	2
(Not in top five*)	64
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116

*"Not in top five" is calculated for reporting purposes based on responses to CAR5. It was not offered as a response option.

CAR6. [CONTINUED.]

Safety	Total
1 Most important	13
2 Second most important	8
3 Third most important	6
4 Fourth most important	4
5 Least important	2
(Not in top five*)	68
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Style	Total
1 Most important	2
2 Second most important	3
3 Third most important	2
4 Fourth most important	2
5 Least important	3
(Not in top five*)	87
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Towing capability	Total
1 Most important	1
2 Second most important	2
3 Third most important	1
4 Fourth most important	2
5 Least important	2
(Not in top five*)	92
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Vehicle comfort	Total
1 Most important	4
2 Second most important	3
3 Third most important	5
4 Fourth most important	6
5 Least important	5
(Not in top five*)	76
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116
Vehicle size	Total
1 Most important	4
2 Second most important	4
3 Third most important	3
4 Fourth most important	4
5 Least important	3
(Not in top five*)	82
Base: All respondents (each respondent only saw items selected in CAR5, but percentages are out of full sample)	2,116

*"Not in top five" is calculated for reporting purposes based on responses to CAR5. It was not offered as a response option.

DENTAL WORK SECOND OPINIONS

DENTAL1. [REQUEST RESPONSE IF LEFT UNANSWERED.]

Have you ever gotten a second opinion on a treatment or procedure recommended by a dentist, such as a filling, a root canal, or a crown?	
	Total
	%
Yes	27
No	73
Base: All respondents	2,115

DENTAL2. [SHOW IF DENTAL1 = 'YES.']

You said that you have gotten a second opinion about a recommended dental procedure. What did you decide to do as a result of the second opinion?	
	Total
	%
Have the procedure	57
Not have the procedure	17
Postpone the procedure	15
Have a different procedure	11
Base: Respondents who got a second opinion	604

BRAINPOWER

BRAIN1. *[[REQUEST RESPONSE IF LEFT UNANSWERED. RANDOMIZE RESPONSE OPTIONS. 'NONE OF THESE' WAS EXCLUSIVE.]]*

Have you noticed yourself or a family member doing any of the following?	
Select <u>all</u> that apply.	
	Total
	%
Yourself	
Forgetting words or names	38
Misplacing frequently-used items, like keys or a cell phone	28
Having trouble finding the right word to describe an object (e.g., "place to put flowers" instead of "flowerpot")	28
Losing interest in hobbies or activities	24
Forgetting appointments or plans made with other people	16
Repeating the same questions, stories, or statements over and over	15
Having problems with judgment (e.g., making bad financial decisions, having trouble making decisions)	12
Misplacing items in unusual places, such as leaving eyeglasses in the refrigerator	11
Forgetting the correct month or year	7
Getting lost in places this person has been before	5
None of these	36
Base: All respondents	2,116
A family member	
	Total
Misplacing frequently-used items, like keys or a cell phone	28
Forgetting words or names	27
Repeating the same questions, stories, or statements over and over	26
Having trouble finding the right word to describe an object (e.g., "place to put flowers" instead of "flowerpot")	19
Forgetting appointments or plans made with other people	17
Having problems with judgment (e.g., making bad financial decisions, having trouble making decisions)	15
Losing interest in hobbies or activities	15
Misplacing items in unusual places, such as leaving eyeglasses in the refrigerator	13
Forgetting the correct month or year	10
Getting lost in places this person has been before	9
None of these	42
Base: All respondents	2,116

BRAIN2A. [SHOW IF ANYTHING BESIDES 'NONE OF THESE' SELECTED IN BRAIN1 FOR 'YOURSELF.' SHOW ALL ITEMS SELECTED IN BRAIN1 FOR 'YOURSELF' IN SAME ORDER AS SHOWN IN BRAIN1.]

You said that you had noticed yourself doing the following. For each one, please indicate if it happens frequently enough that it causes you to worry about your thinking abilities or memory.

Only select if it causes you to worry about your thinking abilities or memory.

	Total
	%
Forgetting words or names	40
Base: Respondents who said they noticed themselves doing this	805
Forgetting appointments or plans made with other people	36
Base: Respondents who said they noticed themselves doing this	329
Having trouble finding the right word to describe an object (e.g., "place to put flowers" instead of "flowerpot")	35
Base: Respondents who said they noticed themselves doing this	592
Getting lost in places I have been before	35
Base: Respondents who said they noticed themselves doing this	108
Forgetting the correct month or year	33
Base: Respondents who said they noticed themselves doing this	150
Losing interest in hobbies or activities	32
Base: Respondents who said they noticed themselves doing this	488
Having problems with judgment (e.g., making bad financial decisions, having trouble making decisions)	31
Base: Respondents who said they noticed themselves doing this	235
Misplacing frequently-used items, like keys or a cell phone	31
Base: Respondents who said they noticed themselves doing this	557
Misplacing items in unusual places, such as leaving eyeglasses in the refrigerator	28
Base: Respondents who said they noticed themselves doing this	221
Repeating the same questions, stories, or statements over and over	23
Base: Respondents who said they noticed themselves doing this	323

BRAIN2A. [COMBINED RESPONSES, SHOWN OUT OF ALL RESPONDENTS.]

You said that you had noticed yourself doing the following. For each one, please indicate if it happens frequently enough that it causes you to worry about your thinking abilities or memory.

Only select if it causes you to worry about your thinking abilities or memory.

	Total
	%
Any of these	34
Base: All respondents	2,116

BRAIN2B. [SHOW IF ANYTHING BESIDES 'NONE OF THESE' SELECTED IN BRAIN1 FOR 'A FAMILY MEMBER.' SHOW ALL ITEMS SELECTED IN BRAIN1 FOR 'A FAMILY MEMBER' IN SAME ORDER AS SHOWN IN BRAIN1.]

You said you had noticed a family member doing the following. Please indicate for which, if any, of these happen to an extent that makes you worried about that person's thinking abilities or memory.

Only select if it causes you to worry about your family member's thinking abilities or memory.

	Total
	%
Repeating the same questions, stories, or statements over and over	58
Base: Respondents who said they noticed a family member doing this	530
Forgetting the correct month or year	49
Base: Respondents who said they noticed a family member doing this	197
Getting lost in places they have been before	47
Base: Respondents who said they noticed a family member doing this	201
Having problems with judgment (e.g., making bad financial decisions, having trouble making decisions)	45
Base: Respondents who said they noticed a family member doing this	310
Misplacing items in unusual places, such as leaving eyeglasses in the refrigerator	41
Base: Respondents who said they noticed a family member doing this	261
Having trouble finding the right word to describe an object (e.g., "place to put flowers" instead of "flowerpot")	41
Base: Respondents who said they noticed a family member doing this	392
Forgetting appointments or plans made with other people	40
Base: Respondents who said they noticed a family member doing this	355
Forgetting words or names	39
Base: Respondents who said they noticed a family member doing this	543
Losing interest in hobbies or activities	38
Base: Respondents who said they noticed a family member doing this	317
Misplacing frequently-used items, like keys or a cell phone	37
Base: Respondents who said they noticed a family member doing this	549

BRAIN2B. [COMBINED RESPONSES, SHOWN OUT OF ALL RESPONDENTS.]

You said you had noticed a family member doing the following. Please indicate for which, if any, of these happen to an extent that makes you worried about that person's thinking abilities or memory.

Only select if it causes you to worry about your family member's thinking abilities or memory.

	Total
	%
Any of these	33
Base: All respondents	2,116

BRAIN3A. [SHOW IF ANYTHING SELECTED IN BRAIN2A. RANDOMIZE RESPONSE OPTIONS, HOLDING 'OTHER' AND 'HAVE NOT DONE ANYTHING' AT END IN THAT ORDER. 'HAVE NOT DONE ANYTHING' WAS EXCLUSIVE.]

You said that you are concerned about your own thinking abilities or memory. Which, if any, of the following have you done to address these issues?

Select all that apply.

	Total
	%
Started doing 'brain training' activities, such as crossword puzzles, sudoku, or memory games	36
Changed routines, such as setting up a place to always put keys or phone	31
Taken brain-boosting supplements	12
Got evaluated for an illness that might affect cognition	12
Other, please specify	4
Have not done anything to address these concerns	36
Base: Respondents who said they have noticed themselves doing at least one of the things we asked about to an extent that worries them	712

BRAIN3B. [SHOW IF ANYTHING SELECTED IN BRAIN2B. RANDOMIZE RESPONSE OPTIONS, HOLDING 'OTHER,' 'HAVE NOT DONE ANYTHING' AND 'DON'T KNOW' AT END IN THAT ORDER. 'HAVE NOT DONE ANYTHING' AND 'DON'T KNOW' WERE EXCLUSIVE.]

You said that you are concerned about a family member's thinking abilities or memory. Which, if any, of the following have they done to address these issues?

Select all that apply.

	Total
	%
Started doing 'brain training' activities, such as crossword puzzles, sudoku, or memory games	25
Got evaluated for an illness that might affect cognition	23
Changed routines, such as setting up a place to always put keys or phone	22
Taken brain-boosting supplements	13
Other, please specify	3
Have not done anything to address these concerns	26
Don't know	17
Base: Respondents who said they have noticed a family member doing at least one of the things we asked about to an extent that worries them	699

BRAIN4A. [SHOW IF BRAIN3A = 'HAVE NOT DONE ANYTHING TO ADDRESS THESE CONCERNS.' RANDOMIZE, HOLDING 'OTHER' AT END.]

You said that you are concerned about your own thinking abilities or memory, but have not done anything to address these concerns. Which, if any, of the following are reasons you have not?

Select all that apply.

	Total
	%
Do not think it is serious enough to intervene	59
Do not feel it is worth the hassle	24
Think it will cost too much	18
Afraid of what I will find out	17
Do not think anything will help	14
Trouble finding a health care provider who speaks my language	6
Other, please specify	5
Base: Respondents who said they have noticed themselves doing at least one of the things we asked about to an extent that worries them but have not done anything about it	235

BRAIN4B. [SHOW IF BRAIN3B = 'HAVE NOT DONE ANYTHING TO ADDRESS THESE CONCERNS.' RANDOMIZE, HOLDING 'OTHER' AND 'DON'T KNOW' AT END IN THAT ORDER. 'DON'T KNOW' WAS EXCLUSIVE.]

You said that you are concerned about a family member's thinking abilities or memory, but they have not done anything to address these concerns. Which, if any, of the following are reasons they have not?

Select all that apply.

	Total
	%
Do not think it is serious enough to intervene	40
I am concerned, but they are not	33
Afraid of what they will find out	13
Do not think anything will help	12
Do not feel it is worth the hassle	10
Think it will cost too much	10
Trouble finding a health care provider who speaks this person's language	1
Other, please specify	7
Don't know	19
Base: Respondents who said they have noticed a family member doing at least one of the things we asked about to an extent that worries them but that this person has not done anything about it	192

BRAIN5A.

Do <u>you</u> have a family history of Alzheimer's or dementia?	
	Total
	%
Yes	26
No	74
Base: All respondents	2,102

BRAIN5B. [SHOW IF ANYTHING BESIDES 'NONE OF THESE' SELECTED IN BRAIN1 FOR 'A FAMILY MEMBER.']

Does the person <u>in your family who you just mentioned</u> have a family history of Alzheimer's or dementia?	
	Total
	%
Yes	24
No	51
Unsure	25
Base: Respondents who said they noticed at least one of the things we asked about in BRAIN1B	1,122

CONTACT:

Kristen Purcell
Chief Research Officer
Kristen.Purcell@consumer.org



[@kristenpurcell](https://twitter.com/kristenpurcell)



Facilitating Fraud:

How Consumers Defrauded on Zelle are Left High and Dry by the Banks that Created It



Prepared by the Office of Sen. Elizabeth Warren

October 2022

Executive Summary

In April 2022, Senator Warren opened an investigation of Zelle and its owner and operator, Early Warning Services, LLC (EWS), after numerous reports indicated that Zelle is a preferred tool of fraudsters and bad actors who abuse Zelle's instantaneous, easy-to-exploit transfers to defraud consumers. Zelle and EWS are owned and operated by a consortium of big banks, who initially refused to turn over any significant information on the extent of fraud on the platform.

At a September 2022 Banking Committee hearing, Senators Warren and Menendez continued to press the banks for this information, and received a commitment from several CEOs that they would provide it to Congress. While JPMorgan Chase and several other banks still refused to make key information about fraud public, several others did provide the information. This report contains the findings of Senator Warren's review of data received to date. It finds that:

- **Fraud and theft are rampant on Zelle – and are increasing.** The big banks that own Zelle market the product by telling their customers that the platform is safe and secure. Bank of America tells its customers that Zelle is “a safe and easy way to send money fast.” Similarly, Wells Fargo tells customers, “Zelle is fast, safe, and convenient.” EWS, Zelle's parent company, brands itself as “innovative,” “collaborative,” and “trustworthy.” But PNC Bank reported that the number of fraud and scam claims from customers increased from 8,848 in 2020, to a pace of over 12,300 in 2022. Similarly, U.S. Bank reported 14,886 fraud and scam claims on Zelle in 2020, and that its customers are on pace to report nearly 45,000 claims in 2022. The four banks that reported the relevant data received scam and fraud claims in excess of \$90 million in 2020, and are on pace to receive scam and fraud claims in excess of \$255 million in 2022.
- **Banks are not repaying the vast majority of cases where customers were fraudulently induced into making payments on Zelle.** Overall, four banks reported 192,878 cases of scams – cases where customers reported being fraudulently induced into making payments on Zelle – involving over \$213.8 million of payments in 2021 and the first half of 2022. In the vast majority of these cases, the banks did not repay the customers that were defrauded. Overall the three banks that provided full data sets reported repaying customers in only 3,473 cases (representing 9.6% of scam claims) and repaid only \$2.9 million (representing 11% of payments).
- **Banks are not repaying customers who contest “unauthorized” Zelle payments – potentially violating federal law and CFPB rules.** Zelle claims to have a “zero liability policy” for cases in which a bad actor gains access to a consumer's Zelle account and uses it to make unauthorized payments, and the Electronic Fund Transfer Act (EFTA) and the Consumer Financial Protection Bureau's (CFPB) “Regulation E” require that the banks repay customers when funds are illegally taken out of their account without authorization. But the data provided by the banks revealed that they reimbursed consumers for only 47% of the dollar amount of cases in which customers reported unauthorized payments on Zelle in 2021 and the first half of 2022.

Big banks own and profit from Zelle, but are failing to make their customers whole for both authorized and unauthorized fraudulent activity on the platform, despite their claims that it is safe and that they have a “zero liability” policy for fraud.

The CFPB has regulatory authority over Zelle and other peer-to-peer platforms including Zelle, and is reportedly considering issuing guidance clarifying the scope of “Regulation E.” The findings of this report show that the agency must move quickly to strengthen and improve rules that prevent consumers from being safe on Zelle, and ensure that banks reimburse them when they are defrauded or their money is stolen.

Introduction

Early Warning Services, LLC (EWS) was created by a partnership of large banks in 1990 to “share data to mitigate deposit losses ...and [create] check deposit and check payment validation products.”ⁱ In 2017, the banks that own EWS – JPMorgan Chase, Wells Fargo, U.S. Bank, PNC, Capital One, Bank of America, and Truist – directed the company to create a peer-to-peer payment platform that could be integrated directly into individual financial institutions.ⁱⁱ That peer-to-peer payment platform, Zelle, is now the most popular such platform in the U.S., processing more money than Venmo and CashApp combined.ⁱⁱⁱ These big banks created, own, operate, and market Zelle through EWS, which brands itself as “innovative,” “collaborative,” and “trustworthy.”^{iv} But numerous reports indicate that Zelle is operating as the preferred tool of fraudsters and other bad actors who abuse Zelle’s instantaneous, easy-to-exploit transfers to steal from and defraud consumers.^v

In April 2022, Senator Warren opened an investigation to determine the extent of fraudulent activity on Zelle, and to understand how the company and the banks that own and operate it make consumers whole when they are defrauded on the platform.^{vi} Senators Warren, Menendez, and Reed wrote to EWS seeking information about the frequency of scams and fraud and the company’s policies on redressing consumers who have been defrauded.^{vii}

The information provided by EWS revealed that an estimated \$440 million was lost by Zelle users through frauds and scams in 2021, but that the banks that participate in the network appear not to have provided sufficient recourse to their customers.^{viii} In particular, EWS’ response indicated that Zelle facilitates fraudulent activity of many kinds.^{ix} That includes activity in which a user’s account is accessed by a bad actor and used to transfer a payment – often called “unauthorized” transactions – and activity in which a user is fraudulently induced into transferring a payment to a bad actor – often referred to by EWS and Zelle-participant banks as “authorized” transactions.^x

Zelle indicated that, consistent with federal rules and regulations, it had “adopted a ‘zero-liability’ approach for any transaction through a Participant Institution on the Zelle Network determined to be unauthorized,” and that its rules require each “Participant Institutio[n] to provide full refunds for Zelle transactions determined to be unauthorized within the meaning of the Electronic Fund Transfer Act (EFTA) and Regulation E.”^{xi} In simple terms, Zelle indicated that it would provide redress for users in cases of unauthorized transfers in which a user’s account is accessed by a bad actor and used to transfer a payment. However, EWS’ response also

indicated that neither Zelle nor its parent bank owners would reimburse users fraudulently induced by a bad actor into making a payment on the platform.

Senators Warren, Menendez, Reed, Brown, Van Hollen, Whitehouse, and Sanders then sent letters to the seven big banks that own and operate Zelle's parent company to determine the extent of the problems with illegal and fraudulent activity, and to determine how banks were helping consumers who lost money on the platform.^{xii}

At nearly every turn, most of the big banks have stonewalled, refusing to provide the information requested by members of Congress. However, Senators Warren and Menendez finally obtained commitments from several of the banks' CEOs that they would provide the information on Zelle to Congress during a Committee on Banking, Housing, and Urban Affairs hearing on September 22, 2022.^{xiii}

JPMorgan Chase has refused to make public the complete data on Zelle fraud and scams, even after its CEO, Jamie Dimon, publicly promised before Congress that his company would provide it.^{xiv} But several other banks, in response to these multiple requests from Senators Warren and Menendez, finally provided useful information. This report contains the results of the analysis of this data conducted by the staff of Senator Warren.

Findings

1. Big Banks Own, Operate, Market, and Profit from Zelle

Zelle's parent company, EWS, is owned and operated by seven of the U.S.' largest banks: JPMorgan Chase, Wells Fargo, Bank of America, U.S. Bank, PNC, Capital One, and Truist.^{xv} EWS markets Zelle as "the fast, safe and easy way to send and receive money."^{xvi} The company encourages banks and credit unions to join the Zelle Network and offer the product to consumers as part of their wider suite of banking services.^{xvii} Indeed, EWS pitches Zelle to the nation's banks and credit unions with data suggesting that "customers using Zelle are more profitable and stay with the financial institution longer" than customers who do not use Zelle.^{xviii} In other words, when banks adopt and offer Zelle and their customers use it, banks profit. According to EWS, banks that offer Zelle to customers save on management costs, earn on customer retention and greater engagement with banking products and services, and "maintain a central role in [customers'/members'] financial lives."^{xix}

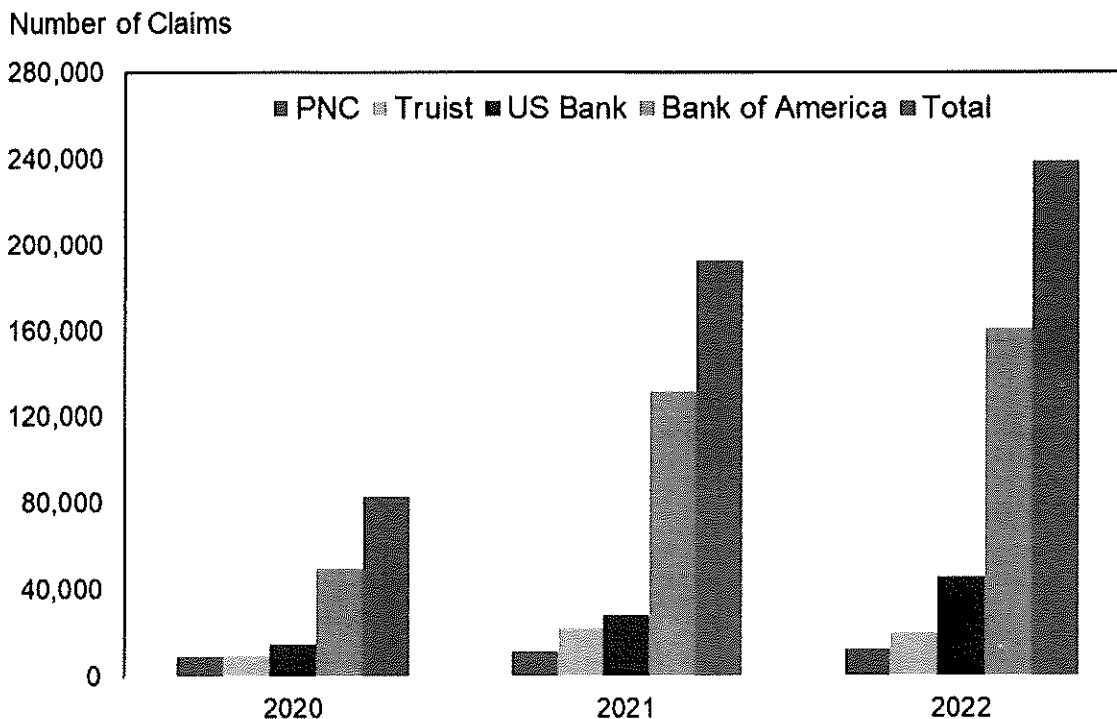
It is in banks' financial interest for consumers to use Zelle. So, while EWS is marketing the Zelle Network to financial institutions, those financial institutions are marketing Zelle to their customers. Six of the seven big banks that own Zelle market the product by telling their customers that the platform is safe or secure.^{xx} Bank of America tells its customers that Zelle is "a safe and easy way to send money fast."^{xxi} Similarly, Wells Fargo tells customers, "Zelle is fast, safe, and convenient."^{xxii}

2. The Volume of Fraudulent Activity on Zelle is Increasing

As Zelle grows in overall volume and market share, consumers across the country continue to share stories of being defrauded and losing money on the platform.^{xxiii} Increasingly, customers are being defrauded through sophisticated deceptions involving a bad actor's use of a reputable institution's name or branding to induce a fraudulent payment – known as “spoofing” – or a bad actor's use of a consumer's own contact information to disguise a payment to the bad actor's account as a payment to the consumer's account – known as “me-to-me.”^{xxiv} Consumers in Massachusetts,^{xxv} Georgia,^{xxvi} Illinois,^{xxvii} and California^{xxviii} have reported being defrauded out of thousands of dollars. In many cases, consumers reported losses that could significantly impact their small business and even wipe out their life savings.^{xxix}

New data provided by the big banks reveals significant increases in the number of fraud and scam claims made by customers over the last two years. For example, PNC Bank reported that the number of claims increased from 8,848 in 2020, to 11,356 in 2021, and that in 2022 the bank's customers are on a pace to report over 12,300 cases of frauds and scams.^{xxx} Similarly, U.S. Bank reported 14,886 fraud and scam claims on Zelle in 2020, and increased to 27,702 in 2021, and that its customers are on pace to report nearly 45,500 in 2022.^{xxxi} Truist reported 9,455 fraud and scam claims on Zelle in 2020, 22,045 in 2021, and that its customers are on pace to report nearly 20,000 in 2022^{xxxii} – a slight decline from 2021, but still well above the number of fraud and scam claims in 2020. Bank of America reported that the number of Zelle fraud and scam claims increased from 49,652 in 2020 to 131,509 in 2021. In 2022, Bank of America customers are on track to report 160,977 incidences of scam and fraud on Zelle.^{xxxiii} Overall, the four banks that provided complete data sets on fraud and scam claims reported a significant increase in the number of fraudulent and scam incidents over the past three years (Figure 1).

Fig. 1: Fraud and Scam Claims on Zelle Are Growing



Note: Chart describes the number of fraud and scam claims reported on Zelle by bank customers. 2022 data is extrapolated from data provided through June 2022. JPMorgan and Wells Fargo did not provide complete data and are excluded from the analysis.

Similarly, the value of fraud and scam claims has increased significantly in recent years. The four banks that provided the relevant data to Senator Warren indicated that the value of scam and fraud claims they received in 2020 was over \$90 million, which jumped by more than 250%, to nearly \$236 million in 2021, and is on pace to exceed \$255 million in 2022.

After receiving numerous requests from Senator Warren, JPMorgan Chase, Wells Fargo, and Capital One failed to provide complete information about the number of cases that were disputed each year and the value of these transactions;^{xxxiv} however, JPMorgan Chase did disclose a total of 335,000 “unauthorized” fraud claims from 2017 to August 2022.^{xxxv} This figure excludes all disputes in which customers reported making deceptively induced payments, which encompasses the popular “spoofing” and “me-to-me” schemes.^{xxxvi}

3. Banks are Not Repaying Consumers Who are Fraudulently Induced by Bad Actors into Making Payments on Zelle

EWS and the banks that run Zelle break fraudulent activity into two categories: ‘fraud’ – which the banks use to “refer to unauthorized transactions, meaning transactions that a consumer does not themselves authorize and initiate (e.g., where a third party obtains the consumer’s access credentials)”^{xxxvii} – and ‘scams,’ which the banks use to refer to transactions that are “authorized

and initiated by a consumer (and thus not unauthorized) but that were induced through deception (e.g., where a third party convinces the consumer to transfer money based on a false pretext, such as an offer to sell nonexistent goods).^{xxxviii}

This is an important distinction, because Zelle indicates that it provides a “zero liability policy” for unauthorized payments, claiming that it reimburses all customers for these cases – but makes no claim or promise to protect customers who are induced by bad actors into making payments.^{xxxix} But the data provided by the banks reveal that fraudulently induced payments are a major problem. For example, Truist, which classifies popular methods like the “me-to-me” and “spoofing” as ‘fraud’ and therefore excludes them from its “zero liability policy,” indicated that customers reported 7,223 cases of scams, involving over \$5.4 million in authorized payments in 2021 and the first half of 2022;^{xl} U.S. Bank reported 21,794 cases, involving over \$13.6 million in scams (authorized payments) in 2021 and the first half of 2022,^{xli} and PNC reported 6,831 cases involving nearly \$6.9 million in authorized payments in the same time period.^{xlii} Bank of America reported 157,030 authorized payments, involving over \$187.9 million in 2021 and the first eight months of 2022.^{xliii}

Overall, the three banks that provided complete data sets – PNC Bank, U.S. Bank, and Truist – reported 35,848 cases of scams, involving over \$25.9 million of payments in 2021 and the first half of 2022. In the vast majority of these cases, the banks did not repay the customers that reported being scammed. Overall these three banks reported repaying customers in only 3,473 cases (representing nearly 10% of scam claims) and repaid only \$2.9 million (representing 11.2% of payments). (Figure 2)

Fig. 2: Banks Refund Only 10% of Zelle Scam Claims

■ % Scam Claims Refunded ■ % Scam Claims Not Refunded



Note: Chart describes the share of Zelle customer scam claims refunded by banks from 2021 through the first half of 2022. Reflects data from PNC Bank, U.S. Bank, and Truist. JPMorgan, Wells Fargo, and Bank of America did not provide complete data and are excluded from the analysis.

4. Banks are Not Repaying Customers Who Contest “Unauthorized” Zelle Payments – Potentially Violating Federal Law and CFPB Rules.

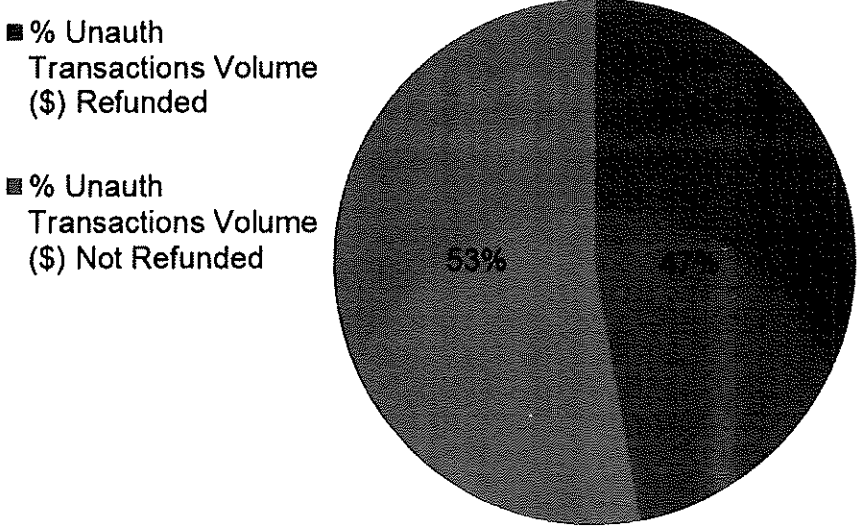
The banks have made a distinction between ‘fraud’ and ‘scam’ claims on Zelle. They generally do not pay consumers back if they are fraudulently induced into making Zelle payments – but claim to repay consumers that suffer unauthorized charges on Zelle. As JPMorgan Chase stated, “we reimburse customers for unauthorized transactions reported in a timely manner.”^{xliv}

Similarly, Wells Fargo stated, “We organize our customer fraud processes in compliance with Regulation E, which provides consumer liability protections and error resolution requirements for electronic fund transfers. In addition to the protections under Regulation E, with timely notification, Zelle customers are not liable for any portion of an unauthorized transaction.”^{xlv}

However, the data provided by the banks reveals that they are not repaying a significant portion of fraud claims. In 2021 and the first six months of 2022, PNC Bank indicated that its customers reported 10,683 cases of unauthorized payments totaling over \$10.6 million, of which only 1,495 cases totaling \$1.46 were refunded to consumers.^{xlvi} PNC Bank left 86% of its customers that reported cases of fraud without recourse for fraudulent activity that occurred on Zelle. Over this same time period, U.S. Bank customers reported a total of 28,642 cases of unauthorized

transactions totaling over \$16.2 million, while only refunding 8,242 cases totaling less than \$4.7 million.^{xlvii} U.S. Bank failed to make over 70% of their consumers whole.^{xlviii} In the period between January 2021 and September 2022, Bank of America customers reported 81,797 cases of unauthorized transactions, totaling \$125 million.^{xlix} Bank of American refunded only \$56.1 million in fraud claims – less than 45% of the overall dollar value of claims made in that time. Truist indicated that the bank had a much better record of reimbursing defrauded customers over this same time period. During 2021 and the first half of 2022, Truist customers filed 24,752 unauthorized transaction claims amounting to \$24.4 million.^l Truist reimbursed 20,349 of those claims, totaling \$20.8 million – 82% of Truist claims were reimbursed over this period.^{li} Overall, however, the four banks that provided complete data sets indicated that they reimbursed only 47% of the dollar amount of fraud claims they received (Figure 3).

Fig. 3: Banks Fail to Refund 53% of Funds Zelle Customers Lose Through Unauthorized Transactions



Note: Chart describes the share of the dollar value of Zelle customer fraud claims refunded by banks between 2021 and the first six months of 2022. Reflects data from PNC Bank, U.S. Bank, Truist, and Bank of America. JPMorgan and Wells Fargo did not provide complete data and are excluded from the analysis.

These data are deeply troubling. They not only reveal that banks are breaking their word about repaying victims harmed by Zelle – they also indicate that the banks may be violating the CFPB’s Regulation E rules, which require banks to make consumers whole after an unauthorized fraudulent transaction.^{lii} That concern is amplified by repeated reports by the CFPB, Federal Reserve Board, and Federal Deposit Insurance Corp. that bank violations of Regulation E’s error resolution rules, including the protection against unauthorized transfers, are common.^{liii}

5. Banks are Refusing to Reveal the True Scope of Fraud and Theft, and the Extent to which they are Repaying Defrauded Customers.

In 2018, just a year after Zelle's introduction as a consumer platform, reports emerged about the product's high volume of fraud. One financial crimes expert told *The New York Times* that, "I know of one bank that was experiencing a 90 percent fraud rate on Zelle transactions, which is insane."^{lv} Despite these reports, consumers and regulators alike had little clarity into the scope of fraudulent activity on Zelle.

In April 2022, following yet another report about "widespread fraud" "flourishing" on Zelle,^{lv} Senators Warren, Menendez, and Reed wrote to EWS requesting information about the rate of fraudulent activity on the platform and the steps taken to recoup losses for consumers.^{lvi} After EWS failed to provide substantive answers,^{lvii} eight Senators wrote to the seven owners of EWS, all of which continuously operated on the platform.^{lviii} Only one bank, Truist, provided any data illustrating the scope of fraud on Zelle, while the other six banks provided failed to produce significant responses.^{lix}

By September 2022, during an appearance in front of the Senate Committee on Banking, Housing, and Urban Affairs, the CEOs of four of EWS' owners claimed they had no knowledge of the fact that Congress and federal bank regulators had requested essential data, only to be stonewalled by their banks.^{lx} JPMorgan Chase CEO Jamie Dimon, PNC Bank CEO William Demchak, U.S. Bancorp CEO Andrew Cecere, and Wells Fargo CEO Charles Scharf committed to "immediately" providing information regarding fraudulent activity on Zelle, and apologized for the delay.^{lxi}

Indeed, during the very same hearing, JPMorgan Chase CEO Jamie Dimon and Wells Fargo CEO Charles Scharf promised Senator Warren that she would have the data she had requested months earlier in hand by the end of the very same day.^{lxii} Four days later, JPMorgan representatives informed Senator Warren's office that they would not provide the information requested by the Senators, while Wells Fargo provided only incomplete and confidential data.^{lxiii}

IV Conclusion

The findings of this report reveal that fraud and theft on Zelle are widespread and growing, with consumers losing millions each year. The banks that own and profit from the platform are failing to make their customers whole for both authorized and unauthorized fraudulent transactions, while refusing to release information publicly or to their customers that could help keep all consumers safe. Given this uncertain landscape and the banks' abdication of responsibility, regulatory clarity is needed to further protect Zelle users.

The CFPB has regulatory authority over peer-to-peer platforms including Zelle, and is reportedly considering issuing guidance to push banks to cover more fraudulently induced transactions, a move that would greatly improve consumer protections on peer-to-peer platforms like Zelle.^{lxiv} The agency should act to clarify and strengthen Regulation E and include fraud in the Regulation's error resolution purview, increasing the responsibility of banks to keep Zelle safe and to ensure that consumers will be protected. The banks that created and profit off of Zelle

should be pushed to protect their consumers from bad actors on their platform, and regulators should step in to ensure a fair and consistent process for everyone.

ⁱ Early Warning Services, LLC, “About,” <https://www.earlywarning.com/about>.

ⁱⁱ Letter from Early Warning Services, LLC to Senators Warren, Menendez, and Reed, May 13, 2022, [On file with the Office of U.S. Senator Elizabeth Warren]; New York Times, “Cash Faces a New Challenger in Zelle, a Mobile Banking Service,” Stacy Cowley, June 12, 2017, <https://www.nytimes.com/2017/06/12/business/dealbook/mobile-banking-zelle-venmo-apple-pay.html>; New York Times, “Fraud is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.

ⁱⁱⁱ Forbes, “Despite A Late Start, Bank-Owned Zelle Moves More Money Than Venmo and Cash App Combined,” Emily Mason, September 8, 2022, <https://www.forbes.com/sites/emilymason/2022/09/08/despite-a-late-start-bank-owned-zelle-moves-more-money-than-venmo-and-cash-app-combined/?sh=7c175ed89d3f>.

^{iv} Letter from Early Warning Services, LLC to Senators Warren, Menendez, and Reed, May 13, 2022, [On file with the Office of U.S. Senator Elizabeth Warren]; Early Warning Services, LLC, website ‘About’ page, <https://www.earlywarning.com/about>; PR Newswire, “Early Warning Appoints Albert Ko as Chief Executive Officer,” May 30, 2019, <https://www.prnewswire.com/news-releases/early-warning-appoints-albert-ko-as-chief-executive-officer-300859164.html>.

^v New York Times, “Fraud Is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.

^{vi} Letter from Senators Warren, Menendez, and Reed to Early Warning Services, LLC CEO Al Ko, April 29, 2022, <https://www.warren.senate.gov/imo/media/doc/2022.04.29%20Letter%20to%20Early%20Warning%20Systems%20LLC.pdf>; Letter from Early Warning Services, LLC to Senators Warren, Menendez, and Reed, May 13, 2022, [On file with the Office of U.S. Senator Elizabeth Warren].

^{vii} *Id.*

^{viii} Letters from Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth to Richard Fairbank, Chairman and CEO of Capital One Financial Corporation, Charles Scharf, CEO and President, Wells Fargo & Co., William S. Demchak, CEO, PNC Financial Services Group. William H. Rogers Jr., CEO, Truist Financial Corporation, Brian T. Moynihan, Chairman and CEO, Bank of America, Andrew J. Cecere, CEO, U.S. Bancorp, Jamie Dimon, Chairman and CEO, JPMorgan Chase & Co., July 7, 2022, <https://www.warren.senate.gov/imo/media/doc/Letters%20to%20Banks%20re%20Zelle.pdf>.

^{ix} Letter from Early Warning Services, LLC to Senators Warren, Menendez, and Reed, May 13, 2022, [On file with the Office of U.S. Senator Elizabeth Warren].

^x Consumer Financial Protection Bureau, “Electronic Fund Transfers FAQs,” December 13, 2021, https://files.consumerfinance.gov/f/documents/cfbp_electronic-fund-transfers-faqs.pdf; Letter from Early Warning Services, LLC to Senators Warren, Menendez, and Reed, May 13, 2022, [On file with the Office of U.S. Senator Elizabeth Warren].

^{xi} Letter from Early Warning Services, LLC to Senators Warren, Menendez, and Reed, May 13, 2022, [On file with the Office of U.S. Senator Elizabeth Warren].

^{xii} Letters from Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth to Richard Fairbank, Chairman and CEO of Capital One Financial Corporation, Charles Scharf, CEO and President, Wells Fargo & Co., William S. Demchak, CEO, PNC Financial Services Group. William H. Rogers Jr., CEO, Truist Financial Corporation, Brian T. Moynihan, Chairman and CEO, Bank of America, Andrew J. Cecere, CEO, U.S. Bancorp, Jamie Dimon, Chairman and CEO, JPMorgan Chase & Co., July 7, 2022, <https://www.warren.senate.gov/imo/media/doc/Letters%20to%20Banks%20re%20Zelle.pdf>.

^{xiii} Senate Committee on Banking, Housing, and Urban Affairs, “Annual Oversight of the Nation’s Largest Banks,” September 22, 2022, <https://www.banking.senate.gov/hearings/annual-oversight-of-the-nations-largest-banks>.

^{xiv} Senate Committee on Banking, Housing, and Urban Affairs, “Annual Oversight of the Nation’s Largest Banks,” September 22, 2022, <https://www.banking.senate.gov/hearings/annual-oversight-of-the-nations-largest-banks>.

^{xv} Letter from Early Warning Services, LLC to Senators Warren, Menendez, and Reed, May 13, 2022, [On file with the Office of U.S. Senator Elizabeth Warren]; Early Warning Services, LLC, “About,” <https://www.earlywarning.com/about>; New York Times, “Cash Faces a New Challenger in Zelle, a Mobile Banking Service,” Stacy Cowley, June 12, 2017, <https://www.nytimes.com/2017/06/12/business/dealbook/mobile-banking-zelle-venmo-apple-pay.html>.

^{xxv} Early Warning Services, LLC, Zelle Product Brief, July 2, 2021, https://www.earlywarning.com/sites/default/files/2021-07/Reseller_Sales_Enablement_Zelle_P2P_Sales_Sheet_07022021_high.pdf.

^{xxvii} *Id.*

^{xxviii} Early Warning Services, LLC, “Explore the Value of Zelle,” <https://www.earlywarning.com/explore-value-zelle>.

^{xix} *Id.*

^{xx} Bank of America, “Send & Receive Money With Zelle,” <https://www.bankofamerica.com/online-banking/mobile-and-online-banking-features/send-receive-money/>; Truist, “Digital Banking,” <https://www.truist.com/digital-banking>; JPMorgan Chase, “Send and Receive Money Fast With Zelle,” <https://www.chase.com/personal/zelle>; U.S. Bank, “Quickly Send and Receive Money With Zelle,” <https://www.usbank.com/online-mobile-banking/zelle-person-to-person-payments.html>; Wells Fargo, “Send and Receive Money,” <https://www.wellsfargo.com/online-banking/zelle/>; Capital One, “Zelle Send Money to Friends and Family,” <https://www.capitalone.com/bank/zelle/>.

^{xxi} Bank of America, website accessed September 27, 2022, <https://www.bankofamerica.com/online-banking/mobile-and-online-banking-features/send-receive-money/>.

^{xxii} Wells Fargo, website accessed September 27, 2022, <https://www.wellsfargo.com/online-banking/zelle/>.

^{xxiii} New York Times, “Fraud Is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.

^{xxiv} *Id.*

^{xxv} Boston 25 News, “‘They’re not robots talking to you. They’re actual people.’ Zelle app users warn of latest scams,” Chris Flanagan, March 23, 2022, <https://www.boston25news.com/news/massachusetts/theyre-not-robots-talking-you-theyre-actual-people-zelle-app-users-warn-latest-scams/WJZVXE23JZFCTPBD5XOPZZXF6I/>.

^{xxvi} WSB-TV, “Customers scammed on Zelle banking app have virtually no fraud protection, consumer advocates say,” Ashli Lincoln, March 22, 2022, <https://www.wsbtv.com/news/local/customers-scammed-zelle-banking-app-have-virtually-no-fraud-protection-consumer-advocates-say/KKSK5LLOWVD47PF2UPTR4IMXSA/>.

^{xxvii} WGN, “As scams soar on Zelle, so does debate over who’s to blame,” Ben Bradley and Andrew Schroedter, March 31, 2022, <https://wgntv.com/news/wgn-investigates/as-scams-soar-on-zelle-so-does-debate-over-whos-to-blame/>.

^{xxviii} ABC 7 News, “LA woman loses over \$18K through ‘Zelle’ after scammers text, call her pretending to be bank,” Carlos Granda, March 12, 2022, <https://abc7.com/los-angeles-zelle-scam-text-message/11644167/>.

^{xxix} WCP0, “Zelle scam steals over \$10,000 from woman,” John Matarese, October 21, 2021, <https://www.wcpo.com/money/consumer/dont-waste-your-money/zelle-scam-steals-over-10-000-from-woman>.

^{xxx} Email from PNC Bank to the Office of Senator Elizabeth Warren, September 23, 2022, [On file with the Office of Senator Elizabeth Warren]; Based on data from January-June 2022, extrapolated to the full calendar year.

^{xxxi} Based on data from January-June 2022, extrapolated to the full calendar year; Email from U.S. Bank to the Office of Senator Elizabeth Warren, September 23, 2022, [On file with the Office of Senator Elizabeth Warren].

^{xxxii} Based on data from January-June 2022, extrapolated to the full calendar year, Letter from Truist to Senators Menendez, Warren, Reed, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren].

^{xxxiii} Letter from Bank of America to the Office of Senator Elizabeth Warren, September 28, 2022, [On file with the Office of Senator Elizabeth Warren].

^{xxxiv} Letters from Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth to Richard Fairbank, Chairman and CEO of Capital One Financial Corporation, Charles Scharf, CEO and President, Wells Fargo & Co., Jamie Dimon, Chairman and CEO, JPMorgan Chase & Co., July 7, 2022, <https://www.warren.senate.gov/imo/media/doc/Letters%20to%20Banks%20re%20Zelle.pdf>; Letters from Senators Warren and Menendez to Jamie Dimon, Chairman and CEO, JPMorgan Chase, Charles Scharf, CEO and President, Wells Fargo & Co., September 22, 2022, <https://www.warren.senate.gov/imo/media/doc/Letters%20to%20Bank%20CEOs.pdf>.

^{xxxv} Letter from JPMorgan Chase to Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth, September 22, 2022, [On file with the Office of Senator Elizabeth Warren].

^{xxxvi} Letter from JPMorgan Chase to Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth, September 22, 2022, [On file with the Office of Senator Elizabeth Warren].

^{xxxvii} Letter from Early Warning Services to Senators Warren, Menendez, and Reed, May 13, 2022, [On file with the Office of U.S. Senator Elizabeth Warren].

^{xxxviii} *Id.*

^{xxxix} *Id.*

-
- ^{xd} Letter from Truist to Senators Menendez, Warren, Reed, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren].
- ^{xd} Email from U.S. Bank to the Office of Senator Elizabeth Warren, September 23, 2022, [On file with the Office of Senator Elizabeth Warren].
- ^{xdii} Email from PNC Bank to the Office of Senator Elizabeth Warren, September 23, 2022, [On file with the Office of Senator Elizabeth Warren].
- ^{xdiii} Letter from Bank of America to the Office of Senator Elizabeth Warren, September 28, 2022, [On file with the Office of Senator Elizabeth Warren].
- ^{xdiv} Letter from JPMorgan Chase to Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren].
- ^{xdiv} Letter from Wells Fargo & Company to Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren].
- ^{xdiv} Email from PNC Bank to the Office of Senator Elizabeth Warren, September 23, 2022, [On file with the Office of Senator Elizabeth Warren].
- ^{xdiv} Email from U.S. Bank to the Office of Senator Elizabeth Warren, September 23, 2022, [On file with the Office of Senator Elizabeth Warren].
- ^{xviii} *Id.*
- ^{xdix} Letter from Bank of America to the Office of Senator Elizabeth Warren, September 28, 2022, [On file with the Office of Senator Elizabeth Warren].
- ⁱ Letter from Truist to Senators Menendez, Warren, Reed, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren].
- ⁱⁱ *Id.*
- ⁱⁱⁱ 15 U.S.C. 1693(g)
- ⁱⁱⁱ See CFPB, Supervisory highlights at 14 (Summer 2021), https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-24_2021-06.pdf (“Supervision continues to find violations of EFTA and Regulation E that it previously discussed in the Fall 2014, Summer 2017, and Summer 2020 editions of Supervisory Highlights, respectively.”); CFPB, Supervisory highlights at 17 (Spring 2022), https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-26_2022-04.pdf (“Examiners continued to find issues with financial institutions failing to follow Regulation E error resolution procedures.”); FDIC, Consumer Compliance Supervisory Highlights (March 2022), <https://www.fdic.gov/regulations/examinations/consumer-compliance-supervisory-highlights/documents/ccs-highlights-march2022.pdf> (listing EFTA violations for failure to properly investigate and resolve errors among the five most recently cited violations in the last year); Federal Reserve System, Consumer Compliance Outlook, Error Resolution and Liability Limitations Under Regulations E and Z: Regulatory Requirements, Common Violations, and Sound Practices (2d Issue 2021), <https://consumercomplianceoutlook.org/2021/second-issue/error-resolution-and-liability-limitations-under-regulations-e-and-z/>.
- ^{liv} New York Times, “Zelle, the Banks’ Answer to Venmo, Proves Vulnerable to Fraud,” Stacy Cowley, April 22, 2018, <https://www.nytimes.com/2018/04/22/business/zelle-banks-fraud.html#:~:text=The%20personal%20payment%20platform%20Zelle,weaknesses%20in%20the%20banks%20security.&text=As%20a%20subscriber%2C%20you%20have.articles%20to%20give%20each%20month>.
- ^{lv} New York Times, “Fraud Is Flourishing on Zelle. The Banks Say It’s Not Their Problem,” Stacy Cowley and Lananh Nguyen, March 6, 2022, <https://www.nytimes.com/2022/03/06/business/payments-fraud-zelle-banks.html>.
- ^{lvi} Letter from Senators Warren, Menendez, and Reed to Early Warning Services, LLC CEO Al Ko, April 29, 2022, <https://www.warren.senate.gov/imo/media/doc/2022.04.29%20Letter%20to%20Early%20Warning%20Systems%20LLC.pdf>.
- ^{lvii} Letter from Early Warning Services to Senators Warren, Menendez, and Reed, May 13, 2022, [On file with the Office of U.S. Senator Elizabeth Warren].
- ^{lviii} Letters from Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth to Richard Fairbank, Chairman and CEO of Capital One Financial Corporation, Charles Scharf, CEO and President, Wells Fargo & Co., William S. Demchak, CEO, PNC Financial Services Group, William H. Rogers Jr., CEO, Truist Financial Corporation, Brian T. Moynihan, Chairman and CEO, Bank of America, Andrew J. Cecere, CEO, U.S. Bancorp, Jamie Dimon, Chairman and CEO, JPMorgan Chase & Co., July 7, 2022, <https://www.warren.senate.gov/imo/media/doc/Letters%20to%20Banks%20re%20Zelle.pdf>.
- ^{lix} Letter from JPMorgan Chase to Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren]; Letter from Wells Fargo & Company to Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth, August

8, 2022, [On file with the Office of Senator Elizabeth Warren]; Letter from Truist to Senators Menendez, Warren, Reed, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren]; Letter from U.S. Bank to Senators Menendez, Warren, Reed, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren];^{lix} Letter from Bank of America to Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren]; Letter from Capital One to Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren]; Letter from PNC to Senators Menendez, Warren, Reed, Brown, Van Hollen, Whitehouse, Sanders, and Duckworth, August 8, 2022, [On file with the Office of Senator Elizabeth Warren].

^{lx} Senate Committee on Banking, Housing, and Urban Affairs, “Annual Oversight of the Nation’s Largest Banks,” September 22, 2022, <https://www.banking.senate.gov/hearings/annual-oversight-of-the-nations-largest-banks>.

^{lxi} Senate Committee on Banking, Housing, and Urban Affairs, “Annual Oversight of the Nation’s Largest Banks,” September 22, 2022, <https://www.banking.senate.gov/hearings/annual-oversight-of-the-nations-largest-banks>; Senator Elizabeth Warren, “At Hearing, Warren Blasts Bank CEOs on Failure to Protect Consumers From Zelle Fraud,” press release, September 22, 2022, <https://www.warren.senate.gov/newsroom/press-releases/at-hearing-warren-blasts-bank-ceos-on-failure-to-protect-consumers-from-zelle-fraud>.

^{lxii} *Id.*

^{lxiii} Phone call between JPMorgan Chase representative and the Office of Senator Elizabeth Warren, September 26, 2022.

^{lxiv} Wall Street Journal, “CFPB to Push Banks to Cover More Payment-Services Scams,” Andrew Ackerman, July 19, 2022, <https://www.wsj.com/articles/consumer-bureau-to-push-banks-to-refund-more-victims-of-scams-on-zelle-other-services-11658235601>.

FLORIDA BAR ETHICS OPINION
OPINION 21-2
March 23, 2021

Advisory ethics opinions are not binding.

A lawyer ethically may accept payments via a Web-based payment-processing service (such as Venmo or PayPal), including funds that are the property of a client or third person, as long as reasonable steps are taken to protect against inadvertent or unwanted disclosure of information regarding the transaction and to safeguard funds of clients and third persons that are entrusted to the lawyer.

RPC: 4-1.1, 4-1.6(a), 4-1.6(e), 4-1.15, 5-1.1(a), (g)

I. Introduction

The Florida Bar Ethics Department has received several inquiries whether lawyers may accept payment from clients via Web-based payment-processing services such as Venmo and PayPal. This also is an increasingly frequent question on the Bar's Ethics Hotline. Accordingly, the Professional Ethics Committee issues this formal advisory opinion to provide Florida Bar members with guidance on the topic.

Several Web-based, mobile, and digital payment-processing services and networks ("payment-processing services") facilitate payment between individuals, between businesses, or between an individual and a business. Some are specifically designed for lawyers and law firms (e.g., LawPay and LexCharge), while others are not (e.g., Venmo, PayPal, ApplePay, Circle, and Square). These services operate in different ways. Some move funds directly from the payor's bank account to the payee's bank account, some move funds from a payor's credit card to a payee's bank account, and some hold funds for a period of time before transferring the funds to the payee. Service fees differ for various transactions, depending on the service's terms of operation. Some offer more security and privacy than others.

The Committee sees no ethical prohibition per se to using these services, as long as the lawyer fulfills certain requirements. Those requirements differ depending on the purpose of the payment—i.e., whether the funds are the property of the lawyer (such as earned fees) or the property of a client or third person (such as advances for costs and fees and escrow deposits). The two principal ethical issues are (1) confidentiality and (2) safeguarding funds of clients and third persons that are entrusted to the lawyer.

II. Analysis

A. Confidentiality

1. The Issue

The use of payment-processing services creates privacy risk. This arises from the potential publication of transactions and user-related information, whether to a network of subscribers or to a population of users interacting with an application. For example, Venmo users, when making a

payment, are permitted to input a description of the transaction (e.g., “\$200 for cleaning service”). Transactions then are published to the feed of each Venmo user who is a party to the transaction. Depending on the privacy settings of each party to the transaction, other users of the application may view that transaction and even comment on it.

For lawyers, accepting payment through a payment-processing service risks disclosure of information pertaining to the representation of a client in violation of Rule 4-1.6(a) of the Rules Regulating The Florida Bar. Rule 4-1.6(a) prohibits a lawyer from revealing information relating to representation of a client absent the client’s informed consent. This prohibition is broader than the evidentiary attorney-client privilege invoked in judicial and other proceedings in which the lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The ethical obligation of confidentiality applies in situations other than those in which information is sought from the lawyer by compulsion of law and extends not only to information communicated between the client and the lawyer in confidence but also to all information relating to the representation, whatever its source. R. Regulating Fla. Bar 4-1.6 cmt. para. [4]. Likewise, a lawyer must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation. *Id.* R. 4-1.6(e); *see also id.* R. 4-1.6 cmt. paras. [24], [25]. The obligation of confidentiality also arises from a lawyer’s ethical duty to provide the client with competent representation. *See id.* R. 4-1.1 cmt. para. [3]. This includes safeguarding information contained in electronic transmissions and communications. *Id.*

Rule 4-1.6(c)(1) permits a lawyer to reveal confidential information to the extent the lawyer reasonably believes necessary to serve the client’s interests. Although receipt of payment in connection with legal services benefits the client, the disclosure of information about the payment to a community of users would not. Wide publication of a Venmo payment “for divorce representation” hardly would serve the client’s interest.¹

2. *Recommended and Required Actions*

Payment-processing services typically offer various privacy settings. Venmo, for example, enables users to adjust their privacy settings to control who sees particular transactions. The options are (1) “Public,” meaning anyone on the Internet will be able to see it, (2) “Friends only,” meaning the transaction will be shared only with the “friends” of the participants to the transaction, and (3) “Private,” meaning it will appear only on the personal feeds of the user and the other participant to the transaction. Venmo has a default rule that honors the more restrictive privacy setting between two users: if either participant’s account is set to Private, the transaction will appear only on the feeds of the participants to the transaction, regardless of the setting enabled by the other participant.²

¹ Revealing to a bank the limited information needed to make a deposit to the lawyer’s account serves the client’s interest. In addition, financial institutions are subject to federal and state laws regarding disclosure of financial information.

² *See* Venmo Help Center, “Payment Activity & Privacy” available at <https://help.venmo.com/hc/en-us/articles/210413717-Payment-Activity-Privacy>.

If, as with Venmo, the service being used permits the recipient to control the privacy setting, the lawyer must select the most secure setting to mitigate against unwanted disclosure of information relating to the representation.

Venmo is only one example of a payment-processing service. Each application has its unique privacy settings and potential risks. The lawyer should be aware that these options can and likely will change from time to time. Prior to using a payment-processing service, the lawyer must diligently research the service to ensure that the service maintains adequate encryption and other security features as are customary in the industry to protect the lawyer's and the client's financial information and to preserve the confidentiality of any transaction. The lawyer must make reasonable efforts to understand the manner and extent of any publication of transactions conducted on the platform and how to manage applicable settings to preempt and control unwanted disclosures. *See* R. Regulating Fla. Bar 4-1.6(e); *id.* R. 4-1.1 cmt. para. [3]. The lawyer must take reasonable steps to avoid disclosure by the lawyer as well as by the client, including advising clients of any steps that they should take to prevent unwanted disclosure of information. Although not ethically required, inserting such advice in the lawyer's retainer or engagement agreement or on each billing statement is wise. For example:

As a convenience to our clients, we accept payment for our services via certain online payment-processing services. The use of these services carries potential privacy and confidentiality risks. Before using one of these services, you should review and elect the privacy setting that ensures that information relating to our representation of you is not inadvertently disclosed to the public at large.

The foregoing is just an example. Variations to fit the circumstances may be appropriate.

These confidentiality obligations apply to any payment that relates to the lawyer's representation of a client, regardless of the purpose of the payment.

B. Safeguarding Funds of Clients and Third Persons

1. The Issue

A customer's account with most payment-processing services such as Venmo and PayPal does not qualify as the type of bank account in which the trust-accounting rules require the funds of clients or third persons in a lawyer's possession be held. Indeed, with limited exceptions, they are not bank accounts at all, rather they are virtual ledgers of funds trading hands, with entries made by the service in the customers' names.

Rule 5-1.1(a)(1) of the Rules Regulating The Florida Bar establishes the fundamental anti-commingling requirement that a lawyer hold in trust, separate from the lawyer's own funds, funds of clients or third persons that are in a lawyer's possession in connection with a representation ("entrusted funds"). It requires that all such funds, including advances for fees, costs, and expenses, "be kept in a separate federally insured bank, credit union, or savings and loan association account maintained in the state where the lawyer's office is situated or elsewhere with the consent of the client or third person and clearly labeled and designated as a trust account."

All nominal or short-term entrusted funds must be deposited in an IOTA account. R. Regulating Fla. Bar 5-1.1(g)(2).³ The IOTA account must be with an “eligible institution,” namely, “any bank or savings and loan association authorized by federal or state laws to do business in Florida and insured by the Federal Deposit Insurance Corporation, any state or federal credit union authorized by federal or state laws to do business in Florida and insured by the National Credit Union Share Insurance Fund, or any successor insurance entities or corporation(s) established by federal or state laws, or any open-end investment company registered with the Securities and Exchange Commission and authorized by federal or state laws to do business in Florida.” *Id.* R. 5-1.1(g)(1)(D).

2. *Recommended and Required Actions*

The Committee concludes that it is permissible for a lawyer to accept entrusted funds via a payment-processing service. To avoid impermissible commingling, the lawyer must maintain separate accounts with the service, one for funds that are the property of the lawyer (such as earned fees), which normally would be deposited in the lawyer’s operating account, and one for entrusted funds (such as advances for costs and fees and escrow deposits), which when in a lawyer’s possession are required to be held in a separate trust account. The lawyer must identify the correct account for the client or third party making the payment.

Rule 5-1.1 applies to funds of clients and third persons that are “in a lawyer’s possession” and requires that any such funds be “kept” in a particular type of account. It does not require that the funds be “immediately” or “directly” deposited into a qualifying account. A payee does not acquire possession—access to and control over—funds transmitted via a payment-processing service until the service makes those funds available in the payee’s account. If the funds are the property of the lawyer, the lawyer may leave those funds in that account or transfer them to another account or payee at the lawyer’s discretion. The lawyer, however, must transfer entrusted funds from the service account into an account at a qualifying banking or credit institution promptly upon their becoming available to the lawyer. By transferring entrusted funds from the service account into a qualified trust account promptly upon acquiring access to and control over those funds, the lawyer complies with the requirement that those funds be *kept* in a qualified account.

Many banks do not permit linking an IOTA account to an account with a payment-processing service such as Venmo or PayPal. In those situations, the lawyer should establish with the banking institution some type of suspense account to which the account established with the payment-processing service can be linked and into which the payments are transferred, then promptly swept into the lawyer’s IOTA account.

Depending upon how quickly the funds are released or other factors, a payment-processing service may charge the payee a transaction fee. Unless the lawyer and the client otherwise agree, the

³ “Nominal or short-term” describes funds of a client or third person that the lawyer has determined cannot earn income for the client or third person in excess of the costs to secure the income. R. Regulating Fla. Bar 5-1.1(g)(1)(A). That determination involves consideration of several factors, such as the amount of the funds and the period of time that the funds are expected to be held. *See id.* R. 5-1.1(g)(3); *see also id.* R. 5-1.1(g)(1)(C) (definition of “IOTA account”).

lawyer must ensure that any such fee is paid by the lawyer and not from client trust funds. Likewise, the lawyer must ensure that any chargebacks are not deducted from trust funds and that the service will not freeze the account in the event of a payment dispute. As with the concern for confidentiality, a lawyer must make a reasonable investigation into a payment-processing service to determine whether the service employs reasonable measures to safeguard funds against loss or theft and has the willingness and resources to compensate for any loss.

III. Conclusion

In sum, the Committee concludes that a lawyer ethically may accept payments via a payment-processing service (such as Venmo or PayPal), including funds that are the property of a client or third person that must be held separately from the lawyer's own funds, under the following conditions:

1. The lawyer must take reasonable steps to prevent the inadvertent or unwanted disclosure of information regarding the transaction to parties other than the lawyer and the client or third person making the payment.

2. If the funds are the property of a client or third person (such as advances for costs and fees and escrow deposits), the lawyer must direct the payor to an account with the service that is used only to receive such funds and must arrange for the prompt transfer of those funds to the lawyer's trust account at an eligible banking or credit institution, whether through a direct link to the trust account if available, through a suspense account with the banking or credit institution at which the lawyer's trust account is maintained and from which the funds automatically and promptly are swept into the lawyer's trust account, or through another substantially similar arrangement.

3. Unless the lawyer and client otherwise agree, the lawyer must ensure that any transaction fee charged to the recipient is paid by the lawyer and not from client trust funds. Likewise, the lawyer must ensure that any chargebacks are not deducted from trust funds and that the service will not freeze the account in the event of a payment dispute.

The Rules of Professional Conduct are "rules of reason" and "should be interpreted with reference to the purposes of legal representation and of the law itself." R. Regulating Fla. Bar ch. 4, pmbl. ("Scope"). When reasonable to do so, the rules should be interpreted to permit lawyers and clients to conduct business in a manner that society has deemed commercially reasonable while still protecting clients' interests. Permitting lawyers to accept payments via payment-processing services under the conditions expressed in this opinion satisfies those objectives.⁴

Note: The discussion about specific applications in this opinion is based on the technology as it exists when this opinion is authored and does not purport to address all such available technology. Web-based applications and technology are constantly changing and evolving. A

⁴The quoted language comes from the Preamble to the Rules of Professional Conduct, which are found in Chapter 4 of the Rules Regulating The Florida Bar. Rule 5-1.1 is part of the Rules Regulating Trust Accounts, which are found in Chapter 5 of the Rules Regulating The Florida Bar). Chapter 5 is incorporated into Chapter 4 by Rule 4-1.15.

lawyer must make reasonable efforts to become familiar with and stay abreast of the characteristics unique to any application or service that the lawyer is using.



Committee on Professional Ethics

Opinion 570 - 6/7/85 (37-84)

Topic: Fee for legal services, advance payment; client, funds of; trust account.

Digest: Fees paid to lawyer in advance of services, refundable to the extent not earned, are not client funds and need not be deposited in trust account; any interest earned on fee advances may be retained by lawyer; upon termination of employment, lawyer must promptly return to client unearned portion of fee paid in advance.

Clarifies N.Y. State
532 (1981)

Code: DR 2-110(A); DR 9-102

QUESTIONS

- (1) Must a lawyer deposit advance payment of legal fees in a trust account as funds of a client, when such payments are refundable to the extent not earned?
- (2) Is a lawyer prohibited from depositing advance payments of legal fees in a trust account as funds of a client?
- (3) Must a lawyer remit to the client interest earned on advance payments of legal fees?

OPINION

A lawyer has adopted the common practice of receiving from a new client advance payment of legal fees expected to be earned in the course of the representation. To the extent that the fees thus advanced are not earned, in whole or in part, during the representation, the lawyer agrees to return them to the client.¹

¹ Although commonly referred to as a "retainer," such an advance payment of legal fees that is not earned until legal services are performed and that is refundable to the extent not earned should be distinguished from the "classic retainer" or "general retainer" more common in earlier times. Such a retainer is a payment to the lawyer for being available to the client in the future and for

(footnote continued)

The lawyer assumes that these advance fee payments are not client funds and that they are not required to be deposited in a client trust account, although it has been the lawyer's practice to deposit them in a trust account nevertheless. The lawyer asks whether she may retain any interest earned on these advance fee payments.

The answer to this inquiry turns upon whether the lawyer is correct in the assumption that advance payments of legal fees are not client funds and are not required to be deposited in a client trust account pursuant to DR 9-102(A). If, contrary to the lawyer's assumption, the fee advances are client funds, it is clear that any interest earned on them belongs to the client and not the lawyer. E.g., ABA 348, at 4-6 (1982); N.Y. State 532 (1981); Nassau County 84-2 (1984); cf. N.Y. City 79-48 (1980).

We conclude that advance payments of legal fees need not be considered client funds and need not be deposited in a client trust account, and that any interest earned on fee advances may therefore be retained by the lawyer. Of course, the lawyer is obliged promptly to return any portion of the fee advance that is not earned in rendering legal services. DR 2-110(A)(3). If the lawyer treats advance payments of fees as the lawyer's own (and therefore retains any interest earned on them), it follows that the lawyer may not deposit the fee advances in a client trust account, as this would constitute impermissible commingling. On the other hand, the lawyer may agree to treat advance payments of legal fees as client funds and deposit them in a client trust account; in that event any interest earned on the funds while in the client trust account must be remitted to the client.

(footnote continued from previous page)

being unavailable to the client's opponents, and is earned upon receipt. See generally Baranowski v. State Bar, 24 Cal. 3d 153, 164 n.4, 593 P.2d 613, 618 n.4, 154 Cal. Rptr. 752, 757 n.4 (1979); Greenberg v. Remick & Co., 230 N.Y. 70, 75, 129 N.E. 211, 212 (1920); Conover v. West Jersey Mortgage Co., 96 N.J. Eq. 441, 451, 126 A. 855, 859 (1924); Bright v. Turner, 205 Ky. 188, 191, 265 S.W. 627, 628 (1924); Union Surety Co. v. Tenny, 200 Ill. 349, 353, 65 N.E. 688, 689 (1902); Severance v. Bizallion, 67 Misc. 103, 106, 121 N.Y.S. 627, 629 (App. T. 1st Dep't 1910); Jacobson v. Sassower, 113 Misc. 2d 279, 281, 452 N.Y.S.2d 981, 983 (Civ. Ct. N.Y. Co. 1982), aff'd, 122 Misc. 2d 862, 474 N.Y.S.2d 167 (App. T. 1st Dep't 1983); H. Drinker, Legal Ethics 172 (1953).

(1) Must Fee Advances Be Deposited in
a Trust Account as Client Funds?

DR 9-102(A) provides:

All funds of clients paid to a lawyer or law firm, other than advances for costs and expenses, shall be deposited in one or more identifiable bank accounts maintained in the state in which the law office is situated and no funds belonging to the lawyer or law firm shall be deposited therein except as follows:

1. Funds reasonably sufficient to pay bank charges may be deposited therein.
2. Funds belonging in part to a client and in part presently or potentially to the lawyer or law firm must be deposited therein, but the portion belonging to the lawyer or law firm may be withdrawn when due unless the right of the lawyer or law firm to receive it is disputed by the client, in which event the disputed portion shall not be withdrawn until the dispute is finally resolved.

Lawyers frequently come into possession of the funds and property of others in a wide variety of situations. They may receive the proceeds of a settlement or judgment, a distribution from an estate or trust, or funds to be distributed upon closing of a real estate conveyance or sale of a business, to mention but a few examples. Such funds clearly are not the property of the lawyer, even though in some circumstances the lawyer's fee may be payable out of them or the lawyer may have a lien upon them to secure payment of a fee.

DR 9-102(A) is an expression of the lawyer's duty, in common with all fiduciaries, to preserve the identity of property belonging to others and not to commingle others' property with the lawyer's own. E.g., Restatement (Second) of Agency §§ 381-82 1207, 1334-35 (1957). Even though DR 9-102(A) by its terms is applicable only to the funds and property of a client, lawyers nevertheless are legally and ethically required to observe the same duty of segregation with respect to the property of third parties. E.g., In re Lurie, 113 Ariz. 95, 98, 546 P.2d 1126, 1129 (1976); Worth v. State Bar, 17 Cal. 3d 337, 341, 551 P.2d 16, 18 (1976); In

re Kramer, 92 Ill. 2d 305, 310, 442 N.E.2d 171, 173 (1982); In re Gallop, 85 N.J. 317, 426 A.2d 509 (1981); N.Y. City 82-8 (1983).

DR 9-102(A) parallels the normal common law rule against commingling, to which specific reference is made in the drafters' notes:

[C]ommingling is committed when a client's money is intermingled with that of his attorney and its separate identity lost so that it may be used for the attorney's personal expenses or subjected to claims of his creditors. . . . The rule against commingling was adopted to provide against the probability in some cases, the possibility in many cases, and the danger in all cases that such commingling will result in the loss of clients' money.

ABA Code of Professional Responsibility DR 9-102 n.10 (1969), quoting Black v. State Bar, 57 Cal. 2d 219, 225-26, 368 P.2d 118, 122 (1962).

Textually, it appears that the drafters of the Code of Professional Responsibility did not consider advance payments of fees to be client funds necessitating their deposit in a trust account. DR 9-102(A) makes no explicit reference to advance fee payments. The Code does make explicit reference to advance fee payments in DR 2-110(A)(3), which requires that any unearned fee advance be promptly refunded upon termination of the representation; it does not require that the advance be deposited in a trust account until earned. Indeed, DR 2-110 treats fee advances and client property as different things. It provides specifically in DR 2-110(A)(2) for the return of all client property to the client upon withdrawal from employment, and then provides separately for the refund of any unearned fee advance in DR 2-110(A)(3).

Nor is there any suggestion in any of the Code's numerous provisions dealing with legal fees or client funds that advance payments of legal fees are deemed client funds to be deposited in a trust account. See generally DR 2-103(C)-(D), 2-106, 2-107, 2-110(A)(3), 3-102, 4-101(C)(4), 5-103(A), 5-106(A); EC 2-8, 2-15 to -25, 2-32, 9-5.

Further it strains the normal meaning of words to interpret the phrase "funds of clients" as embracing advance legal fees paid to the lawyer. Although the lawyer receiving an advance fee payment has a legal and ethical obligation to render the services agreed upon and to refund any unearned portion of the fee

advanced, it does not follow that the advance remains client property until earned. Normally, when one pays in advance for services to be rendered or property to be delivered, ownership of the funds passes upon payment, absent an express agreement that the payment be held in trust or escrow, and notwithstanding the payee's obligation to perform or to refund the payment. The lawyers who drafted the Code should not lightly be assumed to have overlooked these fundamental principles in choosing the language of DR 9-102(A).

We are also mindful that the very reason that many lawyers require advance fee payments in the first place is so that they will not be subject to a client's refusal to pay for legal services after they are rendered. If fee advances were required to be deposited in a client trust account, it would follow that this purpose of requiring advance payment could be easily defeated by a client who, after services are rendered, disputes a justly earned fee. Under DR 9-102(A)(2), the disputed portion of the fee would have to be retained in the client trust account, and would not be available to the lawyer, until the dispute was resolved.²

Our conclusion that legal fees paid in advance need not be considered client funds and therefore need not be deposited in a client trust account is supported by some, albeit a minority, of the ethics committee opinions that have considered this question. D.C. 113 (1982), 110 Daily Washington L. Rptr. 2772 (1982), digested in Lawyers' Man. Prof. Cond. 801:2306 (ABA/BNA) (1984); Fla. 76-27 (1976), Fla. Bar Comm. on Professional Ethics, Selected Opinions 88 (1977), indexed in Maru's Digest No. 10867 (Supp. 1980); Md. 83-62 (1983), digested in Lawyers' Man. Prof. Cond. 801:4330 (ABA/BNA) (1984).

We recognize that our conclusion is contrary to the majority of opinions by other ethics committees that have addressed the issue, which would require that advance payments of legal fees be deposited in a client trust account and retained there until earned. Ind. 4-1977, 21 Res Gestae 402 (1977), indexed in Maru's Digest No. 11061 (Supp. 1980); Mass. 78-11, 63 Mass. L. Rev. 231 (1978), indexed in Maru's Digest No. 11441 (Supp. 1980); Ore. 251

² Of course, even if fees paid in advance are deposited in a lawyer's general account, a client could still dispute, justly or unjustly, whether the fee was earned. The difference is that the lawyer would not be deprived of all use of the funds pending resolution of the dispute, a result that the lawyer and client bargained for at the outset of the representation in agreeing to advance payment of the fee.

(1973), indexed in Maru's Digest No. 9812 (Supp. 1975);³ Tex. 391 (1978), 41 Tex. B.J. 322 (1978), indexed in Maru's Digest No. 12749 (Supp. 1980); Va. 186-A (1981); San Francisco Inf. 1973-14 (1973), indexed in Maru's Digest No. 10669 (Supp. 1980). For the reasons set forth above, we decline to follow these opinions.⁴

Based on the foregoing, we must clarify the dictum in N.Y. State 532, at 3-4 (1981), which refers to "advances for costs, expenses or fees not yet earned," among other things, and states: "Such funds should, of course, be kept in an identifiable client account," citing DR 9-102(A). Insofar as this dictum states that advances for costs and expenses must be kept in a client trust account, it is inconsistent with DR 9-102(A), which specifically exempts "advances for costs and expenses." To the extent this dictum would impose the same requirement upon advances for legal fees, it is contrary to our analysis set forth above.

(2) May Fee Advances Be Deposited in a Trust Account as Client Funds?

As seen from the above analysis, the Code does not require a lawyer to treat advance payments of legal fees as client funds. Nevertheless, we recognize that many lawyers consider it more appropriate to treat advances for unearned fees as client funds until the fees are earned through services rendered. We conclude that DR 9-102(A) does not prohibit lawyers from agreeing with their clients to treat fee advances as client funds and depositing them in a client trust account. Where a lawyer agrees to treat advance fee payments in this manner, all of the requirements of DR 9-102 applicable to client funds and trust accounts would govern. These include the prohibition against withdrawing any portion of the lawyers' fee that is disputed by the client, DR 9-102(A)(2), and all of the detailed accounting, recordkeeping,

³ Ore. 251 cites as support Ore. 205 (1972), indexed in Maru's Digest No. 9766 (Supp. 1975). However, Ore. 205 was withdrawn on December 15, 1972. Maru's Digest at 444 (Supp. 1975).

⁴ We are also aware that a view contrary to that adopted here is taken in the textual portion of the Lawyers' Manual On Professional Conduct, 45:104-05 (ABA/BNA) (1984). The textual material relies on some of the ethics committee opinions cited above and also relies heavily on State v. Hilton, 217 Kan. 694, 538 P.2d 977 (1975). We do not agree with the statements in that textual material as to what the court said or held in State v. Hilton.

and reporting requirements of DR 9-102(B) and of the applicable Appellate Division rules,⁵ with which all lawyers should be familiar.

Absent an agreement to treat an advance fee payment as client property, it would be inappropriate for the lawyer to deposit advance fees in a client trust account, as this would constitute commingling prohibited by DR 9-102(A). Further, once a lawyer agrees to treat a fee advance as client property, the lawyer is bound by that agreement and all of its consequences.⁶

(3) Who Earns Interest on Fee Advances?

If a lawyer does not agree to treat a fee advance as client property, the lawyer may use the money as the lawyer chooses (except that the lawyer may not deposit it in a client trust account), subject only to the requirement that any unearned fee paid in advance be promptly refunded to the client upon termination of the employment. DR 2-110(A)(3). In that case, any interest earned on the advance payment of fees would belong to the lawyer.

If the lawyer agrees to treat an advance fee payment as client property, it follows that any interest earned on it must be reported and remitted to the client. E.g., ABA 348, at 4-6 (1982); N.Y. State 532 (1981); Nassau County 84-2 (1984); cf. N.Y. City 79-48 (1980).

Conclusion

For the reasons stated, and subject to the qualifications set forth above, the questions posed are answered in the negative.

⁵ 22 NYCRR §603.15 (1st Dep't); 22 NYCRR §691.12 (2d Dep't); 22 NYCRR §§1022.5, 1022.7 (4th Dep't).

⁶ We do not consider whether or under what circumstances a lawyer's receipt of fee advances may constitute income subject to taxation.

SELECTED SECTIONS OF THE NEW YORK RULES OF PROFESSIONAL CONDUCT (EFF. 4/1/09)

RULE 1.6:

Confidentiality of Information

- (a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:
- (1) the client gives informed consent, as defined in Rule 1.0(j);
 - (2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or
 - (3) the disclosure is permitted by paragraph (b).

“Confidential information” consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential. “Confidential information” does not ordinarily include (i) a lawyer’s legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates.

- (b) A lawyer may reveal or use confidential information to the extent that the lawyer reasonably believes necessary:
- (1) to prevent reasonably certain death or substantial bodily harm;
 - (2) to prevent the client from committing a crime;
 - (3) to withdraw a written or oral opinion or representation previously given by the lawyer and reasonably believed by the lawyer still to be relied upon by a third person, where the lawyer has discovered that the opinion or representation was based on materially inaccurate information or is being used to further a crime or fraud;
 - (4) to secure legal advice about compliance with these Rules or other law by the lawyer, another lawyer associated with the lawyer’s firm or the law firm;
 - (5) (i) to defend the lawyer or the lawyer’s employees and associates against an accusation of wrongful conduct; or
(ii) to establish or collect a fee; or
 - (6) when permitted or required under these Rules or to comply with other law or court order.

SELECTED SECTIONS OF THE NEW YORK RULES OF PROFESSIONAL CONDUCT (EFF. 4/1/09)

- (c) A lawyer shall exercise reasonable care to prevent the lawyer's employees, associates, and others whose services are utilized by the lawyer from disclosing or using confidential information of a client, except that a lawyer may reveal the information permitted to be disclosed by paragraph (b) through an employee.

RULE 3.3 : Conduct Before a Tribunal

- (a) A lawyer shall not knowingly:
 - (1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;
 - (2) fail to disclose to the tribunal controlling legal authority known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or
 - (3) offer or use evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.
- (b) A lawyer who represents a client before a tribunal and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.
- (c) The duties stated in paragraphs (a) and (b) apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.
- (d) In an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.

SELECTED SECTIONS OF THE NEW YORK RULES OF PROFESSIONAL CONDUCT (EFF. 4/1/09)

- (e) In presenting a matter to a tribunal, a lawyer shall disclose, unless privileged or irrelevant, the identities of the clients the lawyer represents and of the persons who employed the lawyer.

- (f) In appearing as a lawyer before a tribunal, a lawyer shall not:
 - (1) fail to comply with known local customs of courtesy or practice of the bar or a particular tribunal without giving to opposing counsel timely notice of the intent not to comply;
 - (2) engage in undignified or discourteous conduct;
 - (3) intentionally or habitually violate any established rule of procedure or of evidence; or
 - (4) engage in conduct intended to disrupt the tribunal.

RULE 4.1 : Truthfulness In Statements To Others

In the course of representing a client, a lawyer shall not knowingly make a false statement of fact or law to a third person.

**RULE 1.15:
PRESERVING IDENTITY OF FUNDS AND PROPERTY OF OTHERS; FIDUCIARY
RESPONSIBILITY; COMMINGLING AND MISAPPROPRIATION OF CLIENT FUNDS
OR PROPERTY; MAINTENANCE OF BANK ACCOUNTS; RECORD KEEPING;
EXAMINATION OF RECORDS**

(a) Prohibition Against Commingling and Misappropriation of Client Funds or Property.

A lawyer in possession of any funds or other property belonging to another person, where such possession is incident to his or her practice of law, is a fiduciary, and must not misappropriate such funds or property or commingle such funds or property with his or her own.

(b) Separate Accounts.

(1) A lawyer who is in possession of funds belonging to another person incident to the lawyer's practice of law shall maintain such funds in a banking institution within New York State that agrees to provide dishonored check reports in accordance with the provisions of 22 N.Y.C.R.R. Part 1300. "Banking institution" means a state or national bank, trust company, savings bank, savings and loan association or credit union. Such funds shall be maintained, in the lawyer's own name, or in the name of a firm of lawyers of which the lawyer is a member, or in the name of the lawyer or firm of lawyers by whom the lawyer is employed, in a special account or accounts, separate from any business or personal accounts of the lawyer or lawyer's firm, and separate from any accounts that the lawyer may maintain as executor, guardian, trustee or receiver, or in any other fiduciary capacity; into such special account or accounts all funds held in escrow or otherwise entrusted to the lawyer or firm shall be deposited; provided, however, that such funds may be maintained in a banking institution located outside New York State if such banking institution complies with 22 N.Y.C.R.R. Part 1300 and the lawyer has obtained the prior written approval of the person to whom such funds belong specifying the name and address of the office or branch of the banking institution where such funds are to be maintained.

(2) A lawyer or the lawyer's firm shall identify the special bank account or accounts required by Rule 1.15(b)(1) as an "Attorney Special Account," "Attorney Trust Account," or "Attorney Escrow Account," and shall obtain checks and deposit slips that bear such title. Such title may be accompanied by such other descriptive language as the lawyer may deem appropriate, provided that such additional language distinguishes such special account or accounts from other bank accounts that are maintained by the lawyer or the lawyer's firm.

(3) Funds reasonably sufficient to maintain the account or to pay account charges may be deposited therein.

(4) Funds belonging in part to a client or third person and in part currently or potentially to the lawyer or law firm shall be kept in such special account or accounts, but the portion belonging to the lawyer or law firm may be withdrawn when due unless the right of the lawyer or law firm to receive it is disputed by the client or third person, in which event the disputed portion shall not be withdrawn until the dispute is finally resolved.

(c) **Notification of Receipt of Property; Safekeeping; Rendering Accounts; Payment or Delivery of Property.**

A lawyer shall:

(1) promptly notify a client or third person of the receipt of funds, securities, or other properties in which the client or third person has an interest;

(2) identify and label securities and properties of a client or third person promptly upon receipt and place them in a safe deposit box or other place of safekeeping as soon as practicable;

(3) maintain complete records of all funds, securities, and other properties of a client or third person coming into the possession of the lawyer and render appropriate accounts to the client or third person regarding them; and

(4) promptly pay or deliver to the client or third person as requested by the client or third person the funds, securities, or other properties in the possession of the lawyer that the client or third person is entitled to receive.

(d) **Required Bookkeeping Records.**

(1) A lawyer shall maintain for seven years after the events that they record:

(i) the records of all deposits in and withdrawals from the accounts specified in Rule 1.15(b) and of any other bank account that concerns or affects the lawyer's practice of law; these records shall specifically identify the date, source and description of each item deposited, as well as the date, payee and purpose of each withdrawal or disbursement;

(ii) a record for special accounts, showing the source of all funds deposited in such accounts, the names of all persons for whom the funds are or were held, the amount of such funds, the description and amounts, and the names of all persons to whom such funds were disbursed;

(iii) copies of all retainer and compensation agreements with clients;

(iv) copies of all statements to clients or other persons showing the disbursement of funds to them or on their behalf;

(v) copies of all bills rendered to clients;

(vi) copies of all records showing payments to lawyers, investigators or other persons, not in the lawyer's regular employ, for services rendered or performed;

(vii) copies of all retainer and closing statements filed with the Office of Court Administration; and

(viii) all checkbooks and check stubs, bank statements, prenumbered canceled checks and duplicate deposit slips.

(2) Lawyers shall make accurate entries of all financial transactions in their records of receipts and disbursements, in their special accounts, in their ledger books or similar records, and in any other books of account kept by them in the regular course of their practice, which entries shall be made at or near the time of the act, condition or event recorded.

(3) For purposes of Rule 1.15(d), a lawyer may satisfy the requirements of maintaining "copies" by maintaining any of the following items: original records, photocopies, microfilm, optical imaging, and any other medium that preserves an image of the document that cannot be altered without detection.

(e) Authorized Signatories.

All special account withdrawals shall be made only to a named payee and not to cash. Such withdrawals shall be made by check or, with the prior written approval of the party entitled to the proceeds, by bank transfer. Only a lawyer admitted to practice law in New York State shall be an authorized signatory of a special account.

(f) Missing Clients.

Whenever any sum of money is payable to a client and the lawyer is unable to locate the client, the lawyer shall apply to the court in which the action was brought if in the unified court system, or, if no action was commenced in the unified court system, to the Supreme Court in the county in which the lawyer maintains an office for the practice of law, for an order directing payment to the lawyer of any fees and disbursements that are owed by the client and the balance, if any, to the Lawyers' Fund for Client Protection for safeguarding and disbursement to persons who are entitled thereto.

(g) Designation of Successor Signatories.

(1) Upon the death of a lawyer who was the sole signatory on an attorney trust, escrow or special account, an application may be made to the Supreme Court for an order designating a successor signatory for such trust, escrow or special account, who shall be a member of the bar in good standing and admitted to the practice of law in New York State.

(2) An application to designate a successor signatory shall be made to the Supreme Court in the judicial district in which the deceased lawyer maintained an office for the practice of law. The application may be made by the legal representative of the deceased lawyer's estate; a lawyer who was affiliated with the deceased lawyer in the practice of law; any person who has a beneficial interest in such trust, escrow or special account; an officer of a city or county bar association; or counsel for an attorney disciplinary committee. No lawyer may charge a legal fee for assisting with an application to designate a successor signatory pursuant to this Rule.

(3) The Supreme Court may designate a successor signatory and may direct the safeguarding of funds from such trust, escrow or special account, and the disbursement of such funds to persons who are entitled thereto, and may order that funds in such account be deposited with the Lawyers' Fund for Client Protection for safeguarding and disbursement to persons who are entitled thereto.

(h) Dissolution of a Firm.

Upon the dissolution of any firm of lawyers, the former partners or members shall make appropriate arrangements for the maintenance, by one of them or by a successor firm, of the records specified in Rule 1.15(d).

(i) Availability of Bookkeeping Records: Records Subject to Production in Disciplinary Investigations and Proceedings.

The financial records required by this Rule shall be located, or made available, at the principal New York State office of the lawyers subject hereto, and any such records shall be produced in response to a notice or subpoena duces tecum issued in connection with a complaint before or any investigation by the appropriate grievance or departmental disciplinary committee, or shall be produced at the direction of the appropriate Appellate Division before any person designated by it. All books and records produced pursuant to this Rule shall be kept confidential, except for the purpose of the particular proceeding, and their contents shall not be disclosed by anyone in violation of the attorney-client privilege.

(j) Disciplinary Action.

A lawyer who does not maintain and keep the accounts and records as specified and required by this Rule, or who does not produce any such records pursuant to this Rule, shall be deemed in violation of these Rules and shall be subject to disciplinary proceedings.

Comment

[1] A lawyer should hold the funds and property of others using the care required of a professional fiduciary. Securities and other property should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer's business and personal property and, if monies, in one or more trust accounts,

including an account established pursuant to the “Interest on Lawyer Accounts” law where appropriate. *See* State Finance Law § 97-v(4)(a); Judiciary Law § 497(2); 21 N.Y.C.R.R. § 7000.10. Separate trust accounts may be warranted or required when administering estate monies or acting in similar fiduciary capacities.

[2] While normally it is impermissible to commingle the lawyer’s own funds with client funds, paragraph (b)(3) provides that it is permissible when necessary to pay bank service charges on that account. Accurate records must be kept regarding which portion of the funds belongs to the lawyer.

[3] Lawyers often receive funds from which the lawyer’s fee will or may be paid. A lawyer is not required to remit to the client funds that the lawyer reasonably believes represent fees owed to the lawyer. However, a lawyer may not withhold the client’s share of the funds to coerce the client into accepting the lawyer’s claim for fees. While a lawyer may be entitled under applicable law to assert a retaining lien on funds in the lawyer’s possession, a lawyer may not enforce such a lien by taking the lawyer’s fee from funds that the lawyer holds in an attorney’s trust account, escrow account or special account, except as may be provided in an applicable agreement or directed by court order. Furthermore, any disputed portion of the funds must be kept in or transferred into a trust account, and the lawyer should suggest means for prompt resolution of the dispute, such as arbitration. The undisputed portion of the funds is to be distributed promptly.

[4] Paragraph (c)(4) also recognizes that third parties may have lawful claims against specific funds or other property in a lawyer’s custody, such as a client’s creditor who has a lien on funds recovered in a personal injury action. A lawyer may have a duty under applicable law to protect such third party claims against wrongful interference by the client. In such cases, when the third-party claim is not frivolous under applicable law, the lawyer must refuse to surrender the property to the client until the claims are resolved. A lawyer should not unilaterally assume to arbitrate a dispute between the client and the third party, but, when there are substantial grounds for dispute as to the person entitled to the funds, the lawyer may file an action to have a court resolve the dispute.

[5] The obligations of a lawyer under this Rule are independent of those arising from activity other than rendering legal services. For example, a lawyer who serves only as an escrow agent is governed by the applicable law relating to fiduciaries even though the lawyer does not render legal services in the transaction and is not governed by this Rule.



Read our research on: [World Leaders](#) | [Artificial Intelligence](#) | [Science Issues](#)



Pew Research Center

Search [pewresearch.org](#)...



[RESEARCH TOPICS](#) ▾ [ALL PUBLICATIONS](#) [METHODS](#) [SHORT READS](#) [TOOLS & RESOURCES](#) [EXPERTS](#) [ABOUT](#)

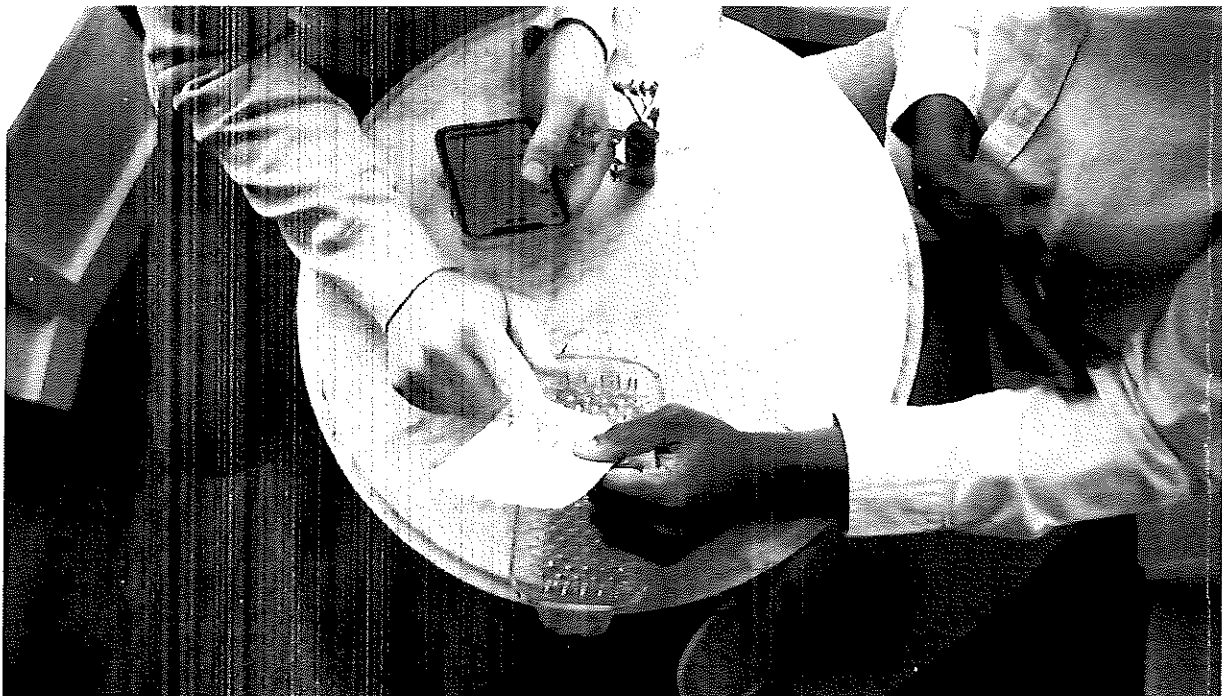
[Home](#) > [Research Topics](#) > [Internet & Technology](#) > [Technology Adoption](#)

SEPTEMBER 8, 2022



Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users

BY MONICA ANDERSON

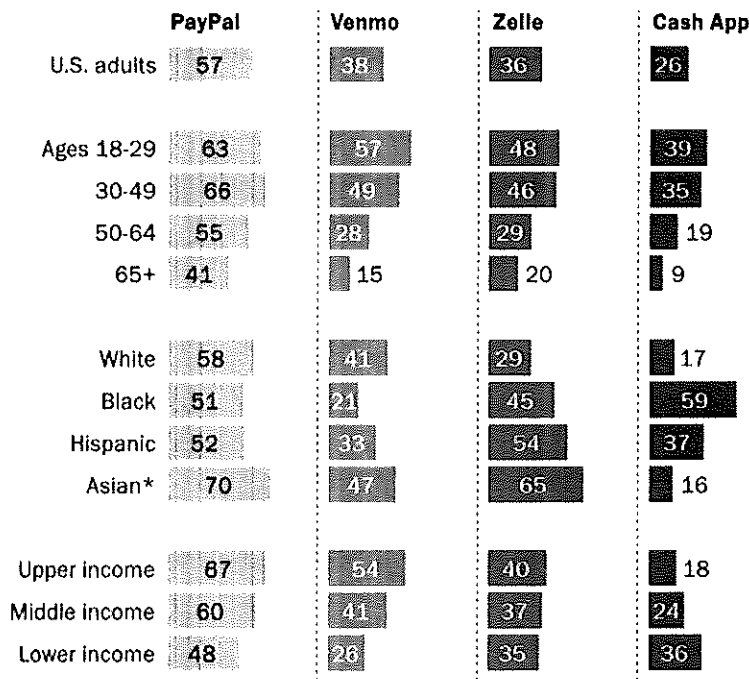


(Tim Scott/Getty Images)

From books to dating, many aspects of life have gone digital, and wallets are no exception. Today, many Americans use the internet and smartphones to transfer money to friends, family and businesses. And while users praise these platforms for making paying for things easier, they also express concerns about security and privacy, according to a new Pew Research Center survey.

Black Americans more likely than other racial, ethnic groups to say they use Cash App; Venmo use varies widely by age, household income

% of U.S. adults who say they ever use the following



* Estimates for Asian adults are representative of English speakers only

Note: Family income tiers are based on adjusted 2020 earnings. White, Black and Asian adults include those who report being only one race and are not Hispanic. Hispanic adults are of any race. Those who did not give an answer are not shown.

Source: Survey of U.S. adults conducted July 5-17, 2022.

PEW RESEARCH CENTER

PayPal – which was founded more than two decades ago – is used by a majority of U.S. adults (57%). Smaller shares report ever using Venmo (38%) or Zelle (36%) and about one-quarter (26%) say they have ever used Cash App, according to the survey, which was conducted July 5-17. In total, 76% of Americans say they have ever used at least one of these four payment sites or apps.

Across each of the platforms measured in the survey, adults under 50 have adopted these tools at higher rates. But the starkest age gap relates to Venmo: 57% of 18- to 29-year-olds report using Venmo, compared with 49% of those ages 30 to 49 and smaller shares among those 50-64 (28%) and 65 and older (15%).

Use of specific payment apps or websites also varies widely by race and ethnicity. For example, 59% of Black Americans say they ever use Cash App, compared with 37% of Hispanic Americans and even smaller shares of White (17%) or Asian Americans (16%). By contrast, Black adults are less likely than other racial or ethnic groups to report being a Venmo user.

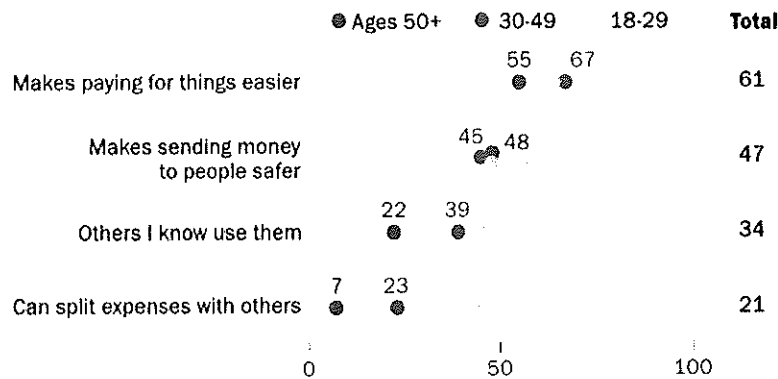
There are also differences by household income. Adults with upper incomes are more likely than middle- and lower-income adults to be users of Venmo or PayPal. In contrast, lower-income adults are the most likely to say they use Cash App: About 36% say this, compared with 24% of middle-income and 18% of upper-income adults.

Why Americans do – or don’t – use these payment sites or apps

When asked what motivates them to use these sites or apps, users most frequently point to ease. Roughly six-in-ten Americans who have ever used PayPal, Venmo, Zelle or Cash App (61%) say a major reason for doing so is because it makes paying for things easier.

A majority of payment app or site users cite it being an easier way of paying as major reason for using; younger users stand out for citing splitting expenses

Among U.S. adults who say they have ever used PayPal, Venmo, Zelle or Cash App, % who say each of the following is a **major reason** they use these payment apps or sites



Note: Those who did not give an answer or who gave other responses are not shown. Source: Survey of U.S. adults conducted July 5-17, 2022.

PEW RESEARCH CENTER

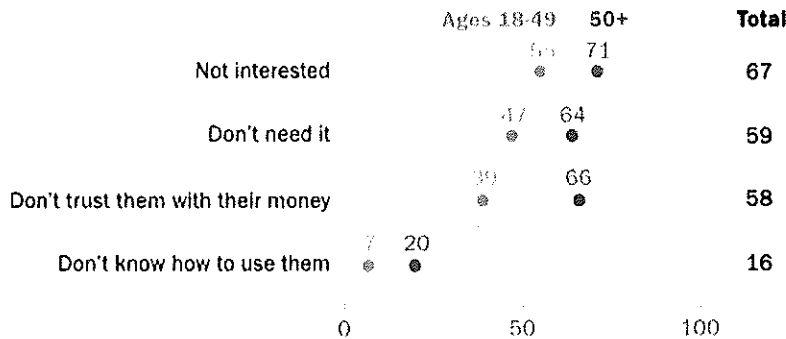
About half of these users (47%) say a key factor for using these platforms is because it makes sending money to people safer. Smaller shares say a major reason they use these platforms is that other people they know use them (34%) or that it allows them to split expenses with others (21%).

Reasons for using these tools vary by age. Some 44% of adults ages 18 to 29 who have used these payment sites or apps cite splitting expenses with others as a major reason, compared with 23% of those ages 30 to 49 and less than one-in-ten for those 50 and older. And users under 50 are more likely than those 50 and older to say a key factor is that other

people they know use these sites or apps.

Older Americans who never use payment apps or sites are especially likely to cite lack of interest, trust as major reasons they forego these platforms

Among U.S. adults who say they have never used PayPal, Venmo, Zelle or Cash App, % who say each of the following is a major reason they do not use these payment apps or sites



Note: Those who did not give an answer or who gave other responses are not shown.
Source: Survey of U.S. adults conducted July 5-17, 2022.

PEW RESEARCH CENTER

While there are a host of reasons why people gravitate toward these payment apps or sites, there is a segment of the public that has never used them. One of the most cited barriers is lack of interest: 67% of Americans who say they have never used PayPal, Venmo, Zelle or Cash App say not being interested is a major reason.

Those who do not have experience with these money-transferring platforms also point to a lack of necessity, as well as distrust. About six-in-ten non-users say a major reason for not using these payment apps or sites is because they don't need them (59%) or because they don't trust them with their money (58%). A much smaller share of this group (16%) cite lack of knowing how to use them as a major reason.

Distrust is a key hindrance for many older Americans. Two-thirds of Americans 50 and older who have never used these payment apps or sites say a major reason for not using them is that they do not trust these platforms with their money. That share drops to 39% among those 18 to 49.

This age pattern appears elsewhere, too: Older non-users are more likely than their younger counterparts to cite not needing these platforms, lack of interest or not knowing how to use them as major reasons why they do not use them.

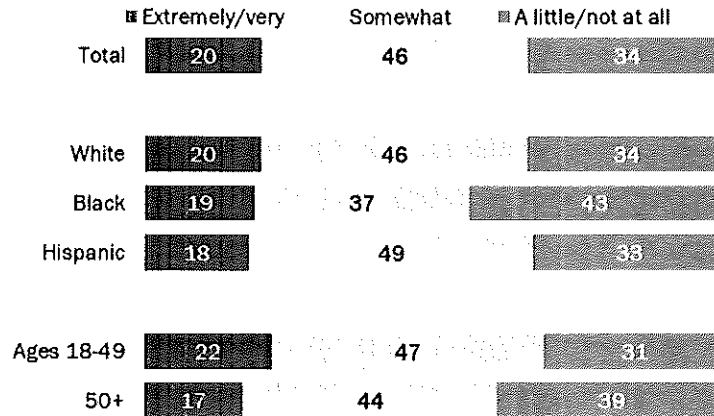
Some lack confidence that payment apps or sites keep consumers' personal information safe

As Americans have turned to digital options to purchase items or transfer money, concerns around security and hacking have followed. This has sparked a larger debate about the vulnerability of payment platforms and whether banks and payment app services have a

responsibility to pay back consumers who have lost money due to fraud.

About a third of payment app or site users say they have little or no confidence that personal information is safe from hackers

Among U.S. adults who say they have ever used PayPal, Venmo, Zelle or Cash App, % who say they are ___ confident that payment apps or sites keep people's information safe from hackers or unauthorized users



Note: White and Black adults include those who report being only one race and are not Hispanic. Hispanic adults are of any race. Those who did not give an answer are not shown. Source: Survey of U.S. adults conducted July 5-17, 2022.

PEW RESEARCH CENTER

The Center's new survey finds mixed views among users on whether these platforms can safeguard people's information from bad actors. About one-third of payment app or site users (34%) say they are a little or not at all confident that payment apps or sites keep people's personal information safe from hackers or unauthorized users.

By comparison, smaller shares of these payment app or site users (20%) say they are extremely or very confident these platforms keep people's information safe from hackers or unauthorized users. The largest share (46%) report they are somewhat confident that payment apps or sites keep personal information away from hackers.

Black users are more skeptical than other groups: 43% say they are only a little or not at all confident that payment sites and apps keep personal information safe from hackers or unauthorized users, compared with about one-third of White or Hispanic users. (There were not enough Asian American payment app or site users to be broken out into a separate analysis.)

There are age differences as well. Adults 50 and older who have ever used these payment sites or apps are more likely than those 18 to 49 to describe their confidence level as a little or not at all confident (39% vs. 31%).

People who have *never* used these payment platforms are highly skeptical that these services keep users' information secure. Roughly eight-in-ten Americans who have never used these payment app or sites say they have a little (20%) or no confidence at all (59%)

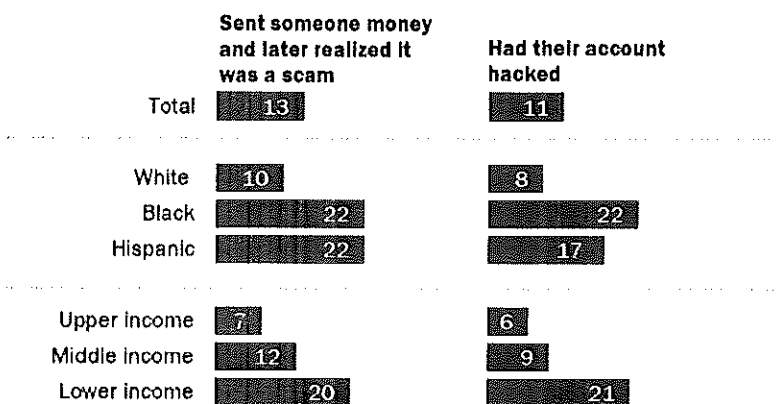
that these services keep people's information safe.

About one-in-ten payment app or site users say they have fallen victim to scams, hacking

Americans' concerns about the safety of their personal data come as some users report personally being the target of scams or hacking.

Black and Hispanic payment app or site users are more likely than those who are White to say they've been scammed, had account hacked

Among U.S. adults who say they have ever used PayPal, Venmo, Zelle or Cash App, % who say they have ever had the following experiences on these payment apps or sites



Note: Family income tiers are based on adjusted 2020 earnings. White and Black adults include those who report being only one race and are not Hispanic. Hispanic adults are of any race. Those who did not give an answer are not shown. Source: Survey of U.S. adults conducted July 5-17, 2022.

PEW RESEARCH CENTER

Some 13% of people who have ever used PayPal, Venmo, Zelle or Cash App say they have sent someone money and later realized it was a scam, while a similar share (11%) report they have had their account hacked.

These negative experiences are more prevalent among certain groups of users. Black and Hispanic Americans who use payment platforms (22% each) are about twice as likely as their White counterparts (10%) to say they have sent money to someone and later realized it was a scam. Black and Hispanic users are also more likely than White users to say they have had their account hacked.

There are also differences by household income. Some 20% of Americans with lower incomes who have ever used these payment apps or sites say they have been the target of this type of a scam, while a similar share say the same about having their account hacked while using these platforms, compared with about one-in-ten or fewer users from middle- or upper-income households. Modest age differences exist, too. For example, 18% of 18- to 29-year-old payment app or site users say they were scammed out of money they sent, compared with 12% of those 30 and older.

Note: Here are the questions, responses and methodology used for this analysis.

Read more from our series examining Americans' experiences with money, investing and spending in the digital age:

- For shopping, phones are common and influencers have become a factor – especially for young adults
- More Americans are joining the 'cashless' economy
- 46% of Americans who have invested in cryptocurrency say it's done worse than expected

Topics Personal Finances, Technology Adoption, Racial & Ethnic Groups Online, E-Commerce

SHARE THIS LINK: <https://pewrsr.ch/3BmYTU2>



Monica Anderson *is a director of research at Pew Research Center.*

POSTS BIO TWITTER EMAIL

Sign up for our weekly newsletter

Fresh data delivered Saturday mornings



Enter email address...

SIGN UP

RELATED

REPORT | JUN 21, 2023

As AI Spreads, Experts Predict the Best and Worst Changes in Digital Life by 2035

SHORT READ | MAY 24, 2023

A majority of Americans have heard of ChatGPT, but few have tried it themselves

SHORT READ | OCT 5, 2022

More Americans are joining the 'cashless' economy

SHORT READ | SEP 8, 2022

Payment apps like Venmo and Cash App bring convenience – and security concerns – to some users

SHORT READ | MAY 4, 2022

As telework continues for many U.S. workers, no sign of widespread 'Zoom fatigue'

TOPICS

Personal Finances

Technology Adoption

E-Commerce

Racial & Ethnic Groups Online


MOST POPULAR

- 1 Quiz: Test your knowledge of digital topics
- 2 32% of Americans have a tattoo, including 22% who have more than one
- 3 What Americans Know About AI, Cybersecurity and Big Tech
- 4 For Most U.S. Gun Owners, Protection Is the Main Reason They Own a Gun
- 5 Why Some Americans Do Not See Urgency on Climate Change

Washington, DC 20036
USA
(+1) 202-419-4300 | Main
(+1) 202-857-8562 | Fax
(+1) 202-419-4372 | Media
Inquiries

[International Affairs](#)

[Economy & Work](#)

 [Instagram](#)

[Immigration & Migration](#)

[Science](#)

 [Twitter](#)


[Race & Ethnicity](#)

[Internet & Technology](#)

 [LinkedIn](#)

[Religion](#)

[News Habits & Media](#)

 [YouTube](#)

[Age & Generations](#)

[Methodological Research](#)

 [RSS](#)

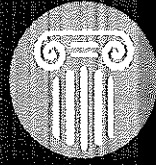
[Gender & LGBTQ](#)

[Full topic list](#)

ABOUT PEW RESEARCH CENTER Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping the world. It conducts public opinion polling, demographic research, media content analysis and other empirical social science research. Pew Research Center does not take policy positions. It is a subsidiary of The Pew Charitable Trusts.

[Copyright 2023 Pew Research Center](#) [About](#) [Terms & Conditions](#) [Privacy Policy](#) [Cookie Settings](#)

[Reprints, Permissions & Use Policy](#) [Feedback](#) [Careers](#)



**South
Carolina
Bar**

ETHICS ADVISORY OPINION

18-05

UPON THE REQUEST OF A MEMBER OF THE SOUTH CAROLINA BAR, THE ETHICS ADVISORY COMMITTEE HAS RENDERED THIS OPINION ON THE ETHICAL PROPRIETY OF THE INQUIRER'S CONTEMPLATED CONDUCT. THIS COMMITTEE HAS NO DISCIPLINARY AUTHORITY. LAWYER DISCIPLINE IS ADMINISTERED SOLELY BY THE SOUTH CAROLINA SUPREME COURT THROUGH ITS COMMISSION ON LAWYER CONDUCT.

South Carolina Rules of Professional Conduct: 1.15

South Carolina Appellate Court Rules: 412, 417

Factual Background:

Licensed South Carolina Lawyer wants to accept earnest money deposits from a client through PayPal.

Questions:

- (1) May a lawyer accept an earnest money deposit through PayPal?
- (2) If a lawyer may accept an earnest money deposit through PayPal, when does the lawyer have to transfer the money from PayPal?

Summary:

Lawyer is required to hold property of clients or third persons in connection with representation separate from the lawyer's own property, but can comply with that obligation if the PayPal account in question does not contain Lawyer's own property and appropriate records are maintained. If the funds received into that account are nominal or short-term funds, Lawyer would then be required to transfer those funds to an IOLTA account for safekeeping, in a manner and timing consistent with Rule 1.15(f) obligations prohibiting disbursement from a trust account until funds are deposited and collected.

Discussion:

Lawyers may receive property of clients or third parties in many different forms. When the property received are funds, the obligation of Lawyer in response is independent of the form in which those funds are received. Regardless of whether funds are received in the form of cash, via check, money order, or credit card, Rule 1.15(a) states “A lawyer shall hold property of clients or third persons that is in a lawyer’s possession in connection with a representation separate from the lawyer’s own property....Other property shall be identified as such and appropriately safeguarded.” As Comment [1] to that rule explains, “A lawyer should hold property of others with the care required of a professional fiduciary.” Lawyers are not restricted to having only one trust account, and any account receiving funds of clients or third parties must be treated as a trust account. “All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer’s business and personal property and, if monies, in one or more trust accounts.” *Id.*

Receipt of funds via an online payment service provider such as PayPal, which allows individuals and businesses to transfer funds electronically to an account maintained with that service provider, trigger the same obligations found in Rule 1.15, RPC and Rule 417, SCAR regarding all other trust accounts. Thus, to adequately maintain the required separation from Lawyer’s own property, such account with any service provider must not contain any funds belonging to the Lawyer. The only exception would be for such amounts as are necessary “for the sole purpose of paying service charges on that account.” Rule 1.15(b).

All trust accounts require extensive documentation be kept current. “Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of six years after termination of the representation.” Rule 1.15(a). Additional financial recordkeeping requirements are contained within Rule 417, SCACR.

Rule 412, SCACR addresses a certain type of trust account, an Interest on Lawyer Trust Accounts (IOLTA), which is likely implicated under the inquirer’s scenario. That rule states that

All nominal or short-term funds belonging to clients or third persons that are placed in trust with any member of the South Carolina Bar practicing law from an office or other business location within the state of South Carolina shall be deposited into one or more IOLTA accounts

Rule 412(b)(1).

“Nominal or short-term” is defined in the rule as funds of a client or third person that “the lawyer has determined cannot provide a positive net return to the client or third person” after consideration of relevant factors outlined in the rule. Rule 412(a)(1) and (d). The “earnest money” referenced by Lawyer in his inquiry likely constitutes “nominal or short-term” funds, and thus those funds initially deposited into the trust account maintained with the online service provider must be moved into Lawyer’s IOLTA trust account.

An additional characteristic of trust accounts generally, however, is a restriction on how and when disbursements therefrom may be made. With an online service provider, transfer from the service provider account into any other account is done via online transfer. Rule 5 within Rule 417, SCACR authorizes electronic transfers from “one client trust account to another client trust account.” However, additional restrictions on disbursements from trust accounts are found in Rule 1.15(f), RPC. That portion of 1.15 states “A lawyer shall not disburse funds from an account containing the funds of more than one client or third person (“trust account”) unless the funds to be disbursed have been deposited in the account and are collected funds.” This requirement is explained as “fundamental to proper trust accounting” in Comment [5] to Rule 1.15.

Certain funds may be treated as collected immediately upon deposit, depending on the manner in which they were received. Rule 1.15(f)(2). Included within the means of deposit that allow for treating the funds as immediately collected is “verified and documented electronic funds transfer.” Rule 1.15(f)(2)(ii). That and other methods listed are identified as “represent[ing] categories of trust account deposits which carry a limited risk of failure so that disbursements may be made in reliance on such deposits without violating the fundamental rule of disbursing only on collected funds.” Comment [7].

However, not all electronic transfers are equal. *See* EAO 12-11 (treating ACH deposits to a trust account as not immediately collected funds due to the reversibility of such deposits, at least until expiration of five banking days after receipt). In this context, online payment service providers such as PayPal have terms of service that are unique to each service provider, subject to change at the provider’s discretion, and which often allow for reversal of credits/payments by clients or third parties to an account on a much more extended timeline than the more heavily-regulated depository institutions that handle traditional checks and “wire transfers.” Thus an “electronic transfer” from an online service provider may not “carry a limited risk of failure” equivalent to more traditional forms of electronic deposit, despite being treated equally under the provisions of Rule 1.15(f)(2).

The risk for the Lawyer in the event of such a reversal of credit/deposit is set forth in Rule 1.15(f)(2), “If the actual collection of deposits described... does not occur, the lawyer shall, as soon as practical but in no event more than five (5) business days after notice of noncollection, deposit replacement funds in the account.”

Accordingly, Lawyer may elect to establish a dedicated trust account via an online payment service provider, but funds received into that account are likely to be nominal or short-term, thus requiring in turn a transfer of those funds to an IOLTA account. Lawyer should be aware of an elevated risk of non-collection under these circumstances in making the individual determination as to whether he is willing to receive funds belonging to third parties via an online payment service provider, PayPal or otherwise.

WASHINGTON STATE BAR ASSOCIATION

Advisory Opinion: 2108

Year Issued: 2005

RPC(s): RPC 1.14

Subject: web-based payment processing service

The Inquirer asks about the ethical propriety of using a web-based payment processing service ("the service") to receive payments from clients. According to the Inquirer, the lawyer initially sets up a web account with the service. Clients then log on to the service's website, and make credit card payments on-line to the lawyer's account. The service immediately notifies the lawyer via email that a payment has been placed into the lawyer's account. The lawyer then enters the account on-line and transfers payment to the correct lawyer's account (trust or operating). We assume that the lawyer will offer the service as an option for account payment, and that it will not be required. We also assume that any cost associated with the service will be paid by the lawyer.

Unlike a traditional credit card arrangement, the client's payment will be placed initially in the lawyer's account with the service. Under RPC 1.14(a), all funds of clients paid to a lawyer or law firm, including advances for costs and expenses, and funds belonging in part to a client and in part presently or potentially to the lawyer or law firm, must be deposited into a trust account meeting the requirements of RPC 1.14(c). Such funds, therefore, must be placed in trust and must not be placed in the lawyer's account with the service for transfer by the lawyer. This is because client funds in the lawyer's account with the service are not safeguarded as required by RPC 1.14.

Assuming that the lawyer investigates the service to determine that accepting payments through it will be reliable and secure, and that the lawyer clearly communicates to the client in advance how the service will work and how payments will be processed by the lawyer, the Committee does not see any ethical problem associated with utilizing the service to collect payments belonging only to the lawyer from clients.

Advisory Opinions are provided for the education of the Bar and reflect the opinion of the Committee on Professional Ethics (CPE) or its predecessors. Advisory Opinions are provided pursuant to the authorization granted by the Board of Governors, but are not individually approved by the Board and do not reflect the official position of the Bar association. Laws other than the Washington State Rules of Professional Conduct may apply to the inquiry. The Committee's answer does not include or opine about any other applicable law other than the meaning of the Rules of Professional Conduct.