Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

April 18, 2022

Digital Wallets and Selected Policy Issues

Digital Wallet Landscape

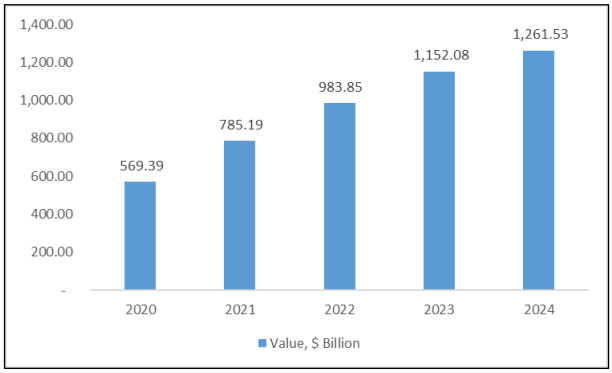
A digital wallet is a software application that stores payment or account details to facilitate traditional payments that use bank and credit card details and/or cryptocurrency transactions. In addition, wallets facilitate peer-to-peer transfers, which have grown rapidly in recent years (**Figure 1**). This In Focus discusses three types of digital wallets and addresses selected policy issues.

Functionality and Scope of Use

Digital wallets are generally used for (1) payments to merchants through the use of near-field communication or QR codes for in-person purchases; (2) peer-to-peer transfers of funds through an app, via text message, or QR codes; (3) storing value from a linked bank account or debit card on an app-based account; or (4) storing, providing access to, and transacting in cryptocurrency. (For more on cryptocurrency, see CRS Report R45427, *Cryptocurrency: The Economics of Money and Selected Policy Issues*.)

Digital wallets generally require the use of internet-connected hardware, such as a smartphone. Some, including Apple Pay and Google Pay, may work only with certain devices and associated operating systems. Others, such as the PayPal or Cash apps, can be downloaded and accessed from a range of devices, irrespective of operating system. For conceptual simplicity, it can be helpful to think of digital wallets as belonging to one of three groups: retailer-specific, general purpose, or cryptocurrency.

Figure 1. Peer-to-Peer Transaction Value



Source: eMarketer, https://www.emarketer.com/content/zelle-records-explosive-q2-growth-faces ... rivals.

Retailer-specific mobile wallets are offered by a retailer for use to purchase its goods and services. They allow individuals to store payment card information, upload funds to digital or registered gift cards, or prefund a balance on an app for future transactions.

General purpose mobile wallets provide much of the same functionality as retail-specific wallets do but are not limited to a specific merchant. For example, someone might use a wallet to make payments at a grocery store, purchase goods online, or pay rent. General purpose mobile wallets include apps tied to a smartphone and those that can be used on any device. Often the companies that provide general purpose wallets are regulated as money transmitters, a state-licensed financial business that moves money between customers.

Cryptocurrency wallets can be divided into three types. *Custodial wallets* are "hosted" or maintained by third-party institutions (such as a crypto exchange). They are funded by bank accounts, and most can be used to buy, sell, or trade certain digital assets. Platforms that host custodial wallets execute digital asset transactions on the account holder's behalf and log them on the custodian's books (or "off-chain") rather than on the distributed ledger blockchain of the coin. *Non-custodial wallets* are not hosted by third-party institutions. They maintain the keys necessary to access and sign the assets for transmission to blockchains and represent the asset's location on the network. Loss of private keys renders cryptocurrency irretrievable. A non-custodial wallet user can transact in crypto without relying on a custodian. *Cold-storage wallets* are pieces of hardware that allow end users to store cryptocurrencies offline, a practice that shields them from hacking. Cold-storage wallets can be connected to the internet to perform transactions.

Policy Considerations for Digital Wallets

Wallets are not themselves accounts or payments but a vehicle for accessing accounts or making payments. Many policy issues that relate to accounts and payments, but not wallets, are often conflated with digital wallet issues. Policy issues highlighted below are specific to wallets.

Data Privacy and Security

Companies offering digital wallets and payments companies generate, and may collect, information about users as part of their business models, raising concerns about privacy and data security. These companies are subject to certain provisions of the Gramm-Leach-Bliley Act (P.L. 106-102) that protect users' nonpublic personal information (NPI). In particular, the act requires the companies to provide privacy notices to consumers about how they use their data and to safeguard the confidentiality of NPI from unauthorized access, but they can typically share information with affiliates and may share information with nonaffiliates unless users opt out.

This policy issue may be addressed through a potential proposed rulemaking for Section 1033 of the Dodd-Frank Act (P.L. 111-203). Section 1033 requires any company or individual offering financial services to provide information it has collected in offering or providing the service to any consumer that requests it. The law, which has not yet been

implemented through rulemaking, would provide consumers with greater access to their financial data and with it the right to take that data and their business elsewhere. Whether this requirement would apply to a digital wallet company remains to be seen.

In October 2021, the Consumer Financial Protection Bureau (CFPB) ordered Amazon, Apple, Facebook, Google, PayPal, and Square to submit information about their payment products to monitor risks to the public and determine whether the operators will "engage in invasive financial surveillance and combine the data they collect on consumers with their geolocation and browsing data" and "use this data to deepen behavioral advertising, engage in price discrimination, or sell to third parties." Some observers have speculated that a CFPB rulemaking may follow.

Consumer Protection and Investor Protection

Mobile wallets. A consumer using a debit, credit, or prepaid card stored on a mobile wallet is protected by the Electronic Funds Transfers Act (P.L. 95-630) and the Truth in Lending Act (P.L. 90-321), implemented through CFPB Regulations E and Z, respectively. Among other things, these regulations establish procedures for resolving errors with unauthorized transactions. Further, consumer credit products offered by wallet companies are regulated as consumer credit whether or not the funds or account information are stored in a digital wallet. Recent rulemakings by the CFPB, such as the 2019 prepaid card rule, effectively extend some of these protections to certain digital wallet transactions.

Funds stored on a wallet are not deposits and are generally not eligible for deposit insurance. However, some wallets provide "pass-through insurance" if a consumer transfers money from a direct deposit to a wallet account. In this scenario, the wallet provider would act as a custodial agent and deposit the money into an FDIC-insured bank account. Where insurance is not offered, policymakers may wish to consider whether wallet users are under the false impression that their wallet balances are insured and whether uninsured balances pose systemic risk.

Crypto wallets. One consideration in the ongoing policy debate is if and how digital asset wallets and the companies that provide them should be regulated and whether the payments regulatory framework should apply to them. Cryptocurrency transactions are not subject to Regulation E primarily because these are not bank products and also because cryptocurrencies are not typically used for consumer payments. As the discussion around whether and to what extent banks may be allowed to participate in cryptocurrency evolves, certain Regulation E protections could be extended to any bank-based cryptocurrency products that are stored in digital wallets or even potentially other cryptocurrencies stored in a bank-issued digital wallet if such a scenario were to emerge.

Digital assets in custodial wallets reside in non-segregated "omnibus accounts" of the digital exchange, which may comingle user and platform assets, unlike a traditional investment account. Market observers have criticized this structure as introducing a principal-agent conflict. Non-segregated accounts could also make it harder for investors to recover assets if an exchange failed or was hacked.

Systemic Risk and Market Power

Mobile wallets. Multilateral standard-setting bodies such as the Bank for International Settlements have suggested that central banks may "need to introduce specific safeguards to guarantee sufficient operational resilience" for companies "offering systemically important payment services to a significant section of the population." While this risk is arguably not material in the United States, "Big Tech" companies offering these services pose a risk because of their size and ability to quickly capture market share. Even if these companies are not systemically important, wallets may provide them with an entree to offer consumers an expanding suite of financial services and products. In addition, commercial (i.e., non-financial) enterprises' entry into payments, which has traditionally been the realm of banking, represents a joining of industries typically kept separate as a matter of long-standing U.S. policy.

The Dodd-Frank Act allows financial institutions and payment systems to be designated as systemically important and subject to heightened prudential standards. It is unclear if this authority could be applied to wallet providers.

Crypto wallets. The President's Working Group's (PWG) report on stablecoins addresses, among other things, systemic risk as it relates to digital asset wallets and stablecoins. The PWG report notes that stablecoins' potential to scale rapidly and inherent run risk could pose systemic risk if one member in the stablecoin arrangement (e.g., a crypto custodian) were to fail or experience distress.

In addition, the PWG report notes that a company both hosting a custodial wallet and issuing a stablecoin could result in an excessive concentration of economic power in the economy and decrease competition. Coinbase—a partner in the issuance of a prominent stablecoin and a large custodial-wallet provider—exemplifies this concern. Among the PWG's recommendations for regulating stablecoins is that custodial wallet holders be subject to "appropriate federal oversight."

Financial Inclusion

Wallets may increase user convenience, but inclusion is an issue of access to accounts, not wallets. Research shows digital payments create alternatives to traditional bank products that can promote financial inclusion among the unbanked, but it typically applies to countries where bank use was not prevalent and alternative accounts or value storage grew in the absence of bank accounts. However, in the United States, where the majority of consumers have access to bank accounts and other financial services, digital wallets may serve only as an ancillary or complementary good. Furthermore, they are typically used on smartphones that the unbanked may not possess.

Paul Tierno, Analyst in Financial Economics
Andrew P. Scott, Analyst in Financial Economics

Disclaimer