HelloWallet

Say Hello to Your Money

HelloWallet Security and Privacy FAQ

You can anticipate that your IT team will want to audit HelloWallet to ensure that is reliable, available, scalable, and secure. This list of frequently asked questions provides an overview of the kinds of questions that a security and privacy team will ask as they perform their due diligence.

Once your IT team is ready to perform their review, HelloWallet will provide a comprehensive Readiness Review packet that answers the questions listed below as well as additional questions in full detail. The Readiness Review Packet provides information regarding policies, technology, and business continuity and is designed to provide complete visibility into HelloWallet's Security and Privacy procedures.

What is HelloWallet?

HelloWallet is a web and mobile application that provides high quality, personalized financial guidance to employees.

Employers receive insight into adoption rates, engagement levels, and the positive financial impact generated by the application. A material ROI comes from supporting program goals (e.g. 401k, HSA) and reducing costs, as well as building a happier and healthier workforce.

HelloWallet has a declarative social mission. For every 5 subscriptions sold, we donate 1 through partnerships with renowned national nonprofits.

Is HelloWallet Cloud-based or Installed? Do we need to integrate with any internal systems?

HelloWallet is software as a service (SaaS). HelloWallet does not require the installation of software on corporate systems or on individual computers. An HelloWallet application for mobile devices can be downloaded by individuals, but the use of this application is not required in order for a user to enjoy the full value of HelloWallet. The HelloWallet the secure associated data are hosted in a secure private cloud.

Do you hold the PCI-DSS Certification (Payment Card Industry Data Security Standard)?

Because HelloWallet does not move or initiate the movement of money, the PCI DSS Certification is not applicable to HelloWallet services. HelloWallet, does, however implement the same level of security policies and procedures created to protect monetary transactions.

The PCI DSS (PCI DSS) was created jointly in 2006 by five major credit-card companies: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. It is a set of policies and procedures designed to ensure the security of debit, cash card and credit card transactions and was created to protect cardholders against misuse of their personal information.

What data are captured by HelloWallet from an individual and from a company?

HelloWallet collects the following information from individuals:

- Registration data such as a user name and password, which are needed to create and access an account.
- Personal information including a person’s name, email address, zip code, and phone number, as well as financial information such as income.

The more information that an individual chooses to share with HelloWallet, the better we are able to customize and provide guidance to meet their needs. It is also important to note that information provided by the individual belongs solely to the individual.

HelloWallet collects the following data from sponsoring companies:

- Employee census data, which includes: name, email address (if available), and a unique identifier such as Employee ID.

How are data protected?

HelloWallet’s security profile is modeled after the widely-recognized ISO-27002 international advisory standard for information security. This standard serves as the foundation of many other information security standards. Dozens of companies have examined and verified our security profile and we are confident in our ability to protect the data entrusted to us. Our third party partners must have an equivalent or better security profile than ours.

Data are protected in transit and at rest. HelloWallet servers present Extended Validation certificates from VeriSign so that users can be sure they are connecting to the authentic HelloWallet service. External vendor communication is over secure channels using RESTful web services over SSL and encrypted SOAP messages.

In addition to being covered by mutual non-disclosure agreements, our partners and enterprise customers exchange data with us using only secure channels. Web service calls are performed using the transport-level security provided by HTTPS over IP-restricted channels. Files are exchanged using Secure FTP after the files are encrypted.

Has HelloWallet ever experienced a data breach?

No, HelloWallet has never experienced data breach.

How does HelloWallet pull in balance and transaction information? What happens after employees enter their bank usernames and passwords?

HelloWallet does not store individual account information anywhere in our operating environment. Account numbers and login credentials provided to HelloWallet by an individual are passed over a secure channel directly to HelloWallet’s account aggregation partner Yodlee. Yodlee makes a connection on behalf of the individual and safeguards that information. Yodlee is used by over 200 financial institutions including Bank of America, Fidelity, and American Express and connects to ~10,000 financial institutions. They are appropriately regulated, reviewed, and certified to handle sensitive financial and personal information.