Frequently asked questions

- Financial apps are incredibly popular, and most banking customers use at least one to make payments, invest, budget, save money, and do a lot more.
- Most financial apps require you to give them your bank and other financial account usernames and passwords so they can access your transactional, investment and other financial information, which potentially might include account profile information, such as your address and cell phone number.
- Consumers can protect and control their data best when they remain aware of which apps are accessing their financial accounts, what information the apps are able to access, whether there is a good reason to access it, and who it's sold to or shared with.
- New ways to control access and safeguard consumer information are available.

Q) How often do the apps that gather my financial account information access my bank accounts?

If they have your bank username and password, then they can access your data whenever they want. Some apps access your account multiple times a day, even if you aren't using the app anymore.

Q) How do I stop a financial app from accessing my financial information?

If you decide to stop using an app, you can contact that app directly to check if it offers the option to disconnect your accounts (just deleting the app will not stop access), or you can simply change your usernames and/or passwords at your bank and other financial institutions you provided it access to.

Q) How do financial apps get my login information? The app I use connects directly to my bank.

For most financial apps, you must provide your bank account username and password to receive services. Some apps use your bank's branding, which may give you the impression that you're logging in through your bank's website, when in fact you're handing over your username and password to a third party. Many apps store this login information (either directly or through a relationship with an aggregator), and it could be compromised if the app has a security breach.

Q) What happens if my financial app has a security breach?

Many financial apps assume only limited responsibility, if any, for security breaches where customer information is compromised, money stolen or fraud committed. Therefore, consumers may not be able to recoup their losses.

Q) How do I know how my financial information is being used?

While they are long and often challenging to understand, reading the financial app's terms and conditions and privacy policy may be the best way to get this information. (See our terms and conditions explainer for some terms that are common in financial app user agreements and what they mean in plain language.)

Q) Can I prevent an app from accessing certain types of financial information?

In most cases, consumers have very little control over the data accessed by financial apps. Most financial apps' terms and conditions don't allow you to specify how your financial information is used, sold or stored. However, some banks offer tools that allow their customers to see which apps are accessing their data, and what data they are receiving.

Q) Which apps are using more secure ways to access financial information?

Some apps are incorporating a "gatekeeper" function that allows them to access only the parts of your information required for the service to run, but not everything in your financial accounts. Some are also implementing safer data sharing practices that put consumers in control of their data. This is done through a partnership with your financial services provider. While this might make your data safer, it doesn't necessarily mean that you won't be liable if there is unauthorized access to your account.

Q) Where can I learn about how FinTech apps work and what "terms and conditions" I am typically agreeing to when I download an app and/or sign up for an account? The apps' policies are usually very long and difficult to understand.

The following are some basic concepts that consumers should be familiar with:

- FinTech apps (financial technology applications): FinTech apps—also known as financial apps—are software platforms that help people manage their finances, budget, make payments, invest, lend or borrow, and carry out other financial tasks. Many FinTech apps that gather your information from different accounts so you can see everything in one place (like Mint), or that initiate payments from your bank account (like Venmo), require users to grant nearly unlimited access to their financial information. Examples of other FinTech apps that require your financial data to work include Square, Cash App, Acorns, LendingClub and Digit.
- Data sharing: Many financial apps require users to give access to their financial information to receive services. Often, checking "Agree" to the terms and conditions gives the app's parent company permission to sell or share the user's information with third parties.
- Data aggregators: These companies provide behind-the-scenes technology used by banks and app developers, functioning as a "middleman" that enables apps to access the financial institution-held customer data. These data aggregators make FinTech functional.
- Screen scraping: Many data aggregators use bots (or similar pieces of software) to sign into financial accounts using the consumer's username and password. Depending on the app, they might have access to data including balances, personal loan information, payments, debts, overdrafts and account statements. Because they use a customer's own login credentials, many data aggregators can check the accounts repeatedly.
- APIs: Application programming interfaces (APIs) exist that allow banks to share information with financial apps without making customers share their login credentials. This is done by creating an interface that allows consumers to log in directly with their bank. With these APIs, banks and other financial services providers can limit the data that is shared to what is required for the app to work, reducing the financial data that is exposed. This allows consumers to take advantage of the app features they want, while keeping their information safer and more secure.

Q) What do I need to know about financial apps?

Stay "security savvy" by knowing that:

- Signing up for a financial app may give the app and/or a behind-the-scenes data aggregator access to much or all of your financial information.
- Financial apps often log in to your account and pull your information through a process called "screen scraping." Depending on the permission it requires users to grant ("terms"), the app and/or a "middleman" (aggregator) might be able to sell or share what it gleans from the accounts you provide access to, including your balances, transaction history, personal loan information, date of birth and contact information. (This is particularly likely with free apps.)
- Some apps request permission to initiate transactions on your behalf through "power of attorney." This permission may be included in the "terms and conditions," which is another reason why you should never agree to the terms without first reading them.

- Responsibility for FinTech-related data breaches and any resulting financial losses can be unclear. Consumers should understand that when they knowingly share usernames and passwords for their accounts, they might not be reimbursed by their bank or the financial app for unauthorized access or transactions.
- Even after you stop using an app and delete it, it might continue to access your bank account information. To cut off any future access, change your usernames and passwords at financial services providers you linked to the app.

Q) What are some steps I can take today to protect my personal financial information and better manage my financial apps?

Here are six tips to be more security savvy:

1. Take an inventory of the financial apps you use or have used. Discontinue service with financial apps you no longer use. Deleting an app may **not** discontinue an app's access to your financial information. One of the easier ways to discontinue service is to change your usernames and passwords at the linked financial institutions so the app can no longer log in to your accounts on your behalf.
2. Regularly change your login credentials. If you don't recall which financial apps you've linked to your bank account(s), simply change your bank username and/or password. Then, reconnect only with those financial apps you still want to use.
3. Read and understand the financial app's terms and conditions. Here you will find important details about how your sensitive information will be used, shared and sold, and whether you are considered responsible for unauthorized access to your linked accounts via the app.
4. Set up alerts and monitor your accounts. Opt in to receive account and security alerts via text or email on all your bank, investment and credit card accounts if your financial services provider offers this functionality. Stay on top of your account balances and pay attention to activity notifications. Check your free credit reports (at AnnualCreditReport.com) to ensure that new accounts or lines of credit haven't been opened in your name.
5. Use strong, unique passwords. Never use the same password and username for your bank account as you do for any other site. Reusing the same login information on different websites, such as social media sites or email, puts your bank accounts at risk, as well as any other accounts using those same credentials.
6. Use "multi-factor authentication" when possible. This is a security option that requires you to verify your identity in some additional way beyond just entering your username and password. Typically, this means receiving a call, email or text message with a one-time passcode every time you sign in to your online or mobile banking account. Access to your account is only approved once you input the single-use passcode. This can seem annoying, but it is a proven method of securing your financial accounts.

Q) Where can I find more information?

Visit the **Share financial data with care** webpage (*http://bit.ly/fintech-privacy*) to view a short video and find more information about how to control and protect your financial information when using apps that require access to your bank and other financial services accounts.

About this guide

This content was developed by Consumer Action and The Clearing House for Consumer Action's Share Financial Data with Care Educational Project.

The Clearing House®