Myth vs. fact: Financial data sharing

In our increasingly digital world, it's a challenge to keep track of who is collecting data about us and how it's being used. FinTech (or financial technology) apps are a popular way to make payments, invest, budget, save money, and do a lot more. Among the most popular are apps that allow users to pull all their financial services accounts into a single place and see all their finances at a glance. Many users give these apps complete access to their bank accounts and financial information when they link up the accounts.

These apps are convenient, but have you ever considered how they make money, since most are free or very low-cost to acquire and use? Many FinTech apps "monetize" their parent companies by selling the financial data they collect from users. During sign-up, users—sometimes unwittingly—may give permission to use their personal and account data in whatever way the app company chooses. On top of that, users sometimes even give the power to initiate transactions via a "power of attorney."

You're probably thinking, "Yes, FinTech apps are convenient, but are they worth giving up my privacy and security?" The good news is, you can enjoy the convenience if you share your bank data with care. Let's bust some common myths about financial data sharing practices!

MYTH: Financial apps just access the specific data required to help me make payments, invest, budget and save money.

FACT: Signing up with a FinTech app may give the app's parent company full access to all your financial information, whether it's needed to provide the intended service or not. Giving access to your bank account by providing your username and password may expose all of your account and transactional information to the app parent company, its affiliates, and the companies it sells data to. This can increase security risks (for example, if any of those companies suffers a security breach or is the victim of a cyberattack).

MYTH: Financial apps only access my data when I am using the app.

FACT: Many financial apps use your stored usernames and passwords to access your account on a regular basis to keep the information they present or use up to date. Some even log into your account several times a day.

MYTH: It's okay to click "Agree" without reading the fine print of the terms and conditions when you sign up for a FinTech app.

FACT: Agreeing to the electronic terms and conditions is the same as signing a contract. Would you sign a contract without reading it? The terms contain important details and conditions about how your sensitive information will be used or shared without further consent. Often, they state that the company has no liability for errors and they prohibit you from suing in court or joining a class action lawsuit.

MYTH: Financial apps don't sell or share data like social media platforms do.

FACT: Financial apps, data aggregators (behind-the-scenes technology that enables apps and banks to "talk" to each other) and social media platforms often have similar business models—they provide you a free or low-cost service by selling client data (which may be aggregated) to other companies or by giving third parties access to you for advertising or promotional purposes. Client data may include your spending, your average credit card balance, how many retirement accounts you have, and more.

MYTH: The financial app I use doesn't have direct access to my data. I log in through my bank.

FACT: Most FinTech apps work by connecting digitally to their users' banks and financial institutions, either to fund transactions or to display account information. *But that doesn't mean you are logging in through your own bank.* Many

FinTech apps rely on contractual relationships with behind-the-scenes technology firms that serve as a link between customers' financial apps and their bank accounts. You may see logos of your bank or other financial services providers in your FinTech app, giving the impression that you are logging in through your bank's website, even though you are actually handing over your username and password to a third party that stores your credentials and has complete access to your bank account information.

MYTH: If there is a security breach, the app is usually responsible for my financial loss.

FACT: Many financial apps assume little to no responsibility for security breaches where customer financial information is compromised, money is stolen, or fraud is committed. Here is an actual disclosure from a popular investing app: "The Company will not be responsible for any losses arising out of the unauthorized use of your account and you agree to indemnify and hold harmless the Company and its managing members, officers, equity holders, employees, partners, parents, subsidiaries, agents, affiliates, and licensors (collectively, "Affiliates"), as applicable, for any improper, unauthorized or illegal uses of your account and as otherwise set forth in these Terms of Use."

To help you use FinTech apps more safely, set up alerts and monitor your bank accounts carefully to catch unauthorized account activity.

MYTH: I deleted my financial app, so now it can't access my financial data anymore.

FACT: Deleting an app is not the same as closing an account. Financial apps might retain access to your usernames and passwords even after you delete them. You need to take steps to actually close the account or cut off its access to any financial accounts you've linked. See if you can revoke access to any accounts you've added by logging in to the app or the company's website before deleting the app. The easiest way to disconnect securely is by revoking your login information or, if that is not possible, changing your usernames and passwords for banking and other accounts you have linked to the app.

MYTH: Using the same password on all my accounts helps me remember what they are.

FACT: It may help you remember, but it is a very risky practice! Use a strong, unique password and username for your bank account. Reusing the same login information on different websites, such as social media sites or email, puts your bank credentials, as well as any other accounts using those same credentials, at risk.

MYTH: Financial apps are convenient, but I am scared to use them because I want to keep my data secure.

FACT: Some apps and financial institutions are working together to use technology that gives apps access to the financial information they need to provide you the services you want without exposing your bank account login credentials. Instead of asking for and storing usernames and passwords, the application program interface—or API—technology uses user-provided account and routing numbers and tokenized digital requests to get information from banks and initiate payments. See our **Frequently Asked Questions** for a breakdown of some common terms to help you determine if FinTech apps are right for you (*https://www.consumer-action.org/downloads/english/FinTech_Savvy_FAQs.pdf*).

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