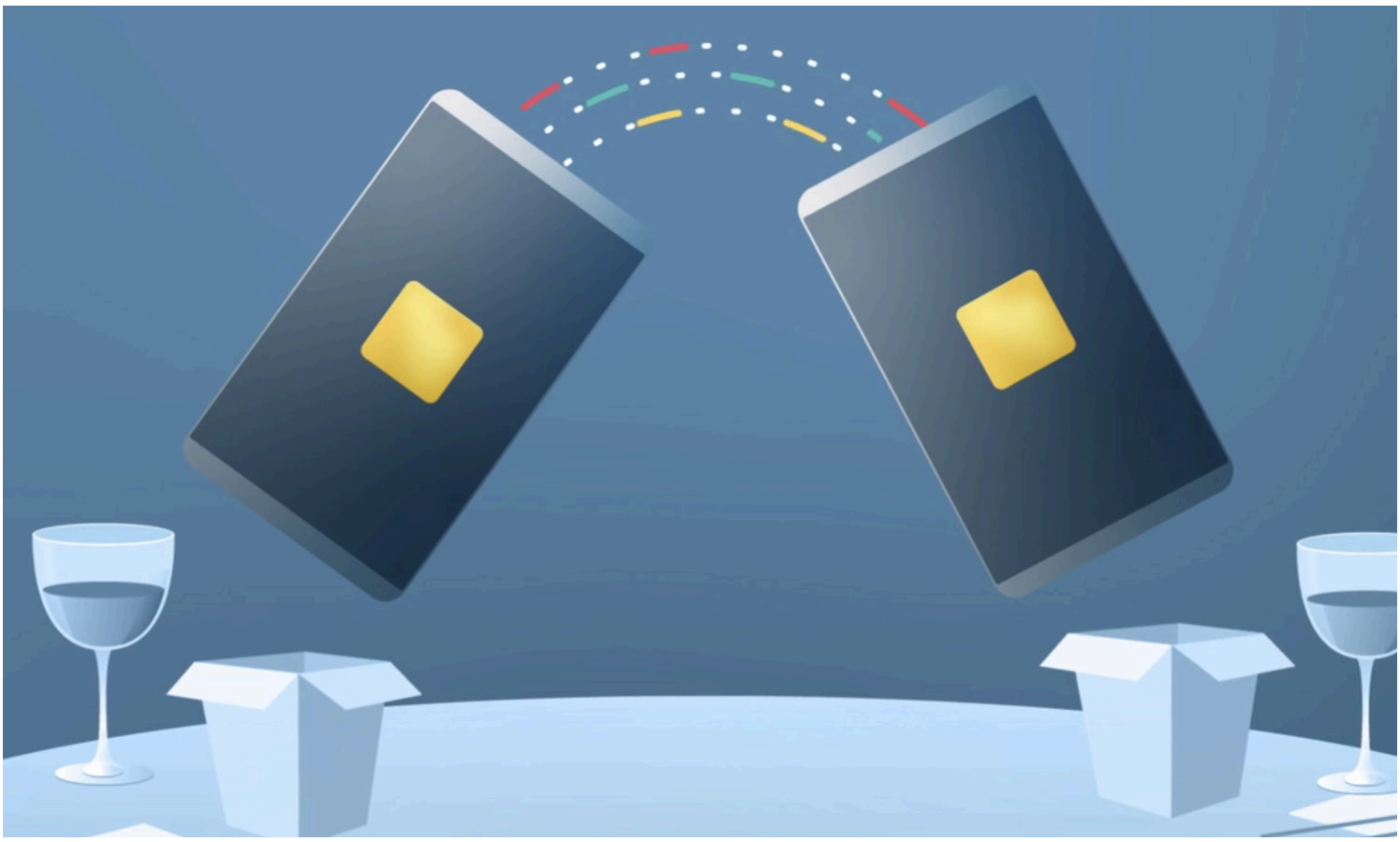
Share financial data with care

Privacy and security when using FinTech apps



When used wisely, financial technology—FinTech—can offer big benefits. Mobile software (apps) and online tools can make managing your finances faster, easier and more convenient. FinTech can even help you achieve your financial goals.

Most FinTech companies place great importance on protecting the privacy and security of their users. Still, it's important that you play an active role in protecting your personal and account information by taking some simple but effective steps when choosing and using FinTech.

Choosing FinTech wisely

While bells and whistles and convenience may be what get your attention, the security of your personal and account information should be your top priority when choosing a FinTech tool.

Wherever you have a financial account (banks, lenders, credit card issuers, investment companies, the Social Security Administration, etc.), the company or agency almost certainly offers its own app or online platform to allow you to access and manage your account. These typically are free, safe and easy to use, with live tech support readily available.

Third-party FinTech apps and tools—those not created for use at a particular financial institution, agency or other entity where you hold an account—require more careful consideration and research because many require you to disclose your bank account username(s) and password(s). While many standalone FinTech tools are reputable and safe, you should shop around and vet

(research) them before choosing one, as you would with any product.

Here are some things to consider:

Privacy policy and security practices: Before downloading a FinTech app or setting up an account, read the company's disclosures—user agreement, privacy policy, terms and conditions, etc.—to find out:

- What type of data it collects
- How, and for how long, the information is stored
- Whether it is sold or shared with others, and for what purposes
- What control—if any—you have over what is collected and how it is used or shared
- What security practices are in place to protect your data
- Who is responsible if there is a data breach and/or you suffer any financial losses
- How you can revoke access to your bank accounts
- If live support is available if you need assistance

If you don't like what you read, choose a different tool. (Here are some tips for "How to Read a Privacy Policy": *https://oag.ca.gov/privacy/facts/online-privacy/privacy-policy*.)

Compatibility and control: If the app or tool you are considering will be linked to your bank accounts, find out if the FinTech company has an agreement with your bank that enables you to control the data it accesses (or revoke access entirely) directly from your bank's dashboard. (You can check with your bank about how it interacts with a particular app, but if you can't determine that ahead of time, you might only be able to find out by signing up and then checking your bank's "security" dashboard, if it has one.) Also try to find out if the app requires you to hand over your account login credentials, or if your login goes directly to your bank. If the app asks for your account information (even if the screen displays what looks like your bank's logo), it means that the app, or a third-party technology provider called a "data aggregator," is storing your bank login information and using it to access your account.

Reputation and responsiveness: Don't download an app unless it comes from a trusted source. Read reviews about any tool you're considering to make sure the developer is legitimate and users are satisfied—both with the tool's functionality and with the way the company handles customer data and resolves any problems. Do an online search for the name of the company or tool along with the word "reviews" or "ratings" to find industry reviews (by companies such as CNET, PCMag.com and TechCrunch), user feedback, or news stories. You can also do an online search for the name along with the keyword "breach" to learn something about the company's security practices, whether it has ever suffered a breach, and, if so, how it responded. However, even well-known apps and those that are reviewed favorably use data aggregators to store your bank login information and can have policies that differ from what you might expect, so you should follow the

privacy and security tips offered below.

Privacy/security tips

There are many FinTech companies that are committed to protecting their users' personal and account information, but online privacy and security is a shared responsibility. Here are some ways that you, as a FinTech consumer, can help reduce potential risks:

Reduce exposure: In the interest of limiting who has access to your data and how many places it is stored (and could be breached), it makes sense to sign up for as few FinTech tools as possible—just enough to meet your needs.

Read the disclosures: These should address all of the questions in the bulleted list above.

Create strong passwords: Use a mix of at least eight numbers, upper- and lower-case letters and symbols. Never use the same password for all your accounts.

Take advantage of added security features: If given the option, enable security measures such as two-factor (or multi-factor) authentication, which requires users to provide two or more pieces of verification (your password plus the answers to security questions, a code sent to your cell phone, or your fingerprint, for example).

Use your bank's dashboard (and/or other resources) to manage FinTech access: If you have an account with one of the growing number of banks that provide a platform where certain apps can be managed from a dashboard, use it to discover what data is being collected by which apps, limit that data to certain accounts and/or certain types of information, or even revoke the app's access entirely. You can also contact the bank if you have questions about the data being collected from your accounts, or if you need help with security.

Opt in to receive notifications from your bank and your FinTech tools: This will keep you in the loop about current security threats, software updates (with security patches), changes to the company's privacy policy or other terms, and account activity that could indicate fraud (for example, notification of a transfer from one of your accounts that you didn't make).

Lock out apps you no longer use: While it's always wise to delete any FinTech apps you no longer use, that's not enough to prevent them from continuing to access your account data. The single most effective way to do this is to change the username and password for your financial accounts. Once you've made the change, you can provide the new username and password to only those apps and tools that you still wish to do business with. (Your bank may have enabled such a feature on its security dashboard, so check there, too.)

Monitor your accounts: Regardless of whether you use FinTech or not, it's wise to check your financial account activity regularly so that you can spot any suspicious activity.

Lock your device and apps: Set your mobile devices (and computer) to require a password or PIN to start or wake up. (Learn how to do this on Apple [*https://support.apple.com/en-ph/HT204060*] and Android [*https://support.google.com/android/answer/9079129*] devices.) Log out of your accounts and/or apps when you're not using them. Turn on features or install apps that can locate, lock or erase your device remotely in case it is lost or stolen.

When something goes wrong

While many FinTech companies make it a top

priority to protect their users' data, they remain largely unregulated, which means that they are not required to implement the same strict security measures that the financial services industry is obligated to use. It also means that there is ambiguity about who—if anyone—is liable when something goes wrong.

When you share your banking username and password with anyone—including a FinTech company—you are handing over the keys to your account(s).

Here are some tips for avoiding, and resolving, problems:

- Send money through peer-to-peer (P2P) mobile payment apps (for example, Venmo and Cash App) and bank money transfer services (such as Zelle) only to people you know and trust. These payments are processed instantly—like using cash—so there's no way to recover your money if you've been scammed or you accidentally sent it to someone with the same name as your intended recipient.
- If something goes wrong (you think you've been scammed, you sent money to the wrong person, or you've sent the wrong amount) do contact your bank and mobile payment company to find out if anything can be done. Some P2Ps may mediate a dispute (but won't reimburse you if the other side doesn't agree to refund your money). Your bank might provide similar help or offer advice.
- Change the passwords for both your bank account and the FinTech account as soon as you notice any unusual or unauthorized activity on your account. If you still want to use the FinTech tool after the problem has been investigated and resolved, you can relink the accounts.
- If your problem cannot be resolved directly, file a complaint with the Consumer Financial Protection Bureau (CFPB) (*https://www.consumerfinance.gov/complaint/*), which will forward it to the company and expect the company to respond to you. You can also file a complaint with the Better Business Bureau (BBB) (*https://www.bbb.org/consumer-complaints/file-a-complaint/get-started*); companies accredited by the organization are required to respond to consumer complaints.

To understand how FinTech works, including why, how and when apps and tools access your financial account information, read Consumer Action's companion guide, **Share financial data with care: What you need to know about how FinTech apps work** (*https://consumer-action.org/english/articles/fintech_apps*).

Visit our **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 Consumer Action

www.consumer-action.org

Through education and advocacy, Consumer Action fights for strong consumer rights and policies that promote fairness and financial prosperity for underrepresented consumers nationwide.

Consumer advice and assistance: Submit consumer complaints to: *www.consumer-action.org/hotline/complaint_form/* or 415-777-9635. (Spanish-language complaints can be submitted to: *https://complaints.consumer-action.org/forms/spanish-form/*.)

Our hotline accepts calls in Chinese, English and Spanish.

About this guide

This guide was created as part of Consumer Action's Share Financial Data with Care Educational Project, with input from The Clearing House.

The Clearing House