WHAT COMES BETWEEN
YOUR FAVORITE FINANCIAL APP AND YOUR BANK ACCOUNT?

PNC knows our customers appreciate the convenience of financial apps that help them to make payments and to manage their finances and investments. PNC is also committed to helping to protect our customers' data and assets. That's why we're taking steps to ensure that our customers who link their PNC account to financial apps understand why and how their data, including sensitive information that could facilitate fraud, might be stored and potentially accessed by third parties.

FINANCIAL TECHNOLOGY FIRMS, APPS, DATA AGGREGATORS AND YOUR PERSONAL DATA

Financial apps that are created and owned by financial technology firms, or fintechs, function by linking their apps to the financial institutions where customers have accounts. Customers using financial apps typically have to provide the fintech firm with their secure online banking login credentials (username and password). For financial apps to perform as intended, fintechs must be connected digitally to the banks and financial institutions where app customers have accounts.

Making digital connections with the myriad of banks and financial institutions used by customers is a large and costly prospect. Fintechs manage this process by contracting with data aggregators — behind-the-scenes technology companies that serve as a link between customers' financial apps and their bank accounts.

What many financial app users do not realize, as outlined in a recent research study conducted by The Clearing House, is that once they provide their secure online banking login credentials to a financial app, data aggregators use this information to log in to customer bank accounts.

Once in the accounts, data aggregators download or "scrape" account information, such as balances, account numbers, transactions and account statements, which is then shared with the fintech that owns the mobile app.

The information "scraped" and maintained by the aggregator, however, may go beyond what is necessary for the particular financial app to fulfill the service requested by the customer, and the data may be maintained by the aggregator even after the customer ceases using the financial app.

The fact that the sensitive information outlined previously is maintained by an outside party is concerning. Of particular concern to us is the storage of account numbers by a third party because fraudsters, if armed with this information, would have the access they need to move money from our customer accounts.

PNC SUPPORTS SECURE FINANCIAL APP USE AND IS COMMITTED TO HELPING PROTECT CUSTOMERS

PNC has implemented enhanced security controls specifically designed to help protect customers' financial accounts and related information when using financial apps that conduct screen scraping.

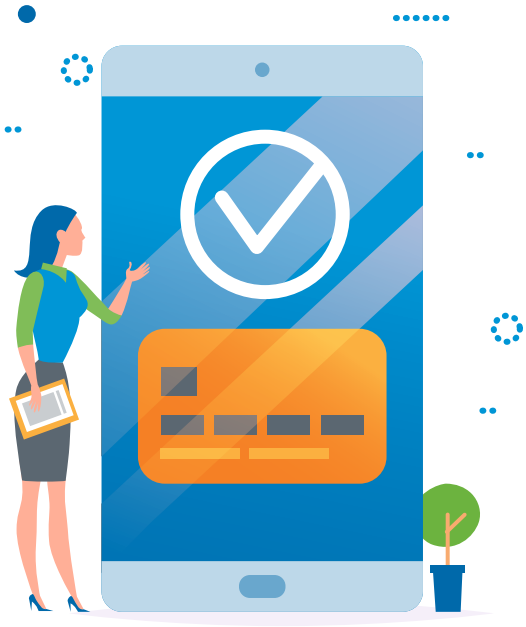
When you connect your PNC account to a financial app, PNC will prompt you to enter a one-time passcode to proceed, and we will send you an alert to confirm that you have initiated the request.

We've also taken steps to protect highly sensitive information that could facilitate fraud or account takeover.

We are collaborating with The Clearing House and Financial Data Exchange, as well as with data aggregators and fintechs, to enable an easy and more secure way to provide access to this data with clear and transparent customer consent.

BANKING CUSTOMERS WHO USE MOBILE APPS SHOULD ASK THE PROVIDER THE FOLLOWING QUESTIONS

- What third-party data aggregator does this financial app use to connect to my bank account?
- What type of data does the aggregator collect when connecting with my bank account?
- Does the data aggregator use encryption when retrieving my data?
- How long will my data be retained by the data aggregator once my use of the financial app has been terminated?
- How do I request that the data aggregator stop collecting my financial data?
- What is the data aggregator's process of purging my data?
- Does the data aggregator share my online banking credentials or other personal and financial information with others, including other service providers?
- What type of liability does the financial app or data aggregator bear in the event of any loss due to a data breach, other unauthorized access or fraud?



BANKING CUSTOMERS CAN USE THE FOLLOWING TIPS TO HELP KEEP THEIR DATA SECURE

USE MULTIFACTOR AUTHENTICATION

This is a security option that allows you to receive a text message with a one-time passcode every time you sign on to your online or mobile banking account. It is an additional step to entering your PNC Online and/or Mobile Banking user ID and password. Access to your account is approved only once you input the one-time passcode.

PNC USER ID AND PASSWORD

If you don't recall what financial apps you've linked to your PNC account, change your PNC Online and/or Mobile Banking user ID and/or password. Then reconnect with financial apps that you actively use with the new user ID and/or password. Never use the same password and user ID to conduct your PNC banking as you do for any other site. Re-using the same login credentials on different websites, such as social media sites or email, puts your credentials at risk, as well as any other account using those same credentials.

READ THE FINE PRINT

A financial app's terms of service agreement often contains important details about the responsibility of the data aggregator and how sensitive information that you provide will be used.

MONITOR YOUR ACCOUNTS

Regularly check your accounts for any unauthorized transactions, including any debits from your account that you did not make or recognize.

SET UP ALERTS

Opt in to receive account and security alerts via text or email on all of your bank, investment and credit card accounts. Stay on top of your account balances, and pay attention to notifications of activity on your account.

NEED HELP?

Need help linking your PNC accounts to an online or mobile financial service?

Learn more about linking your PNC account(s) to an online or mobile financial service ››

CON PDF 1219-058

PNC BANK