Securing Participant Data on Fidelity Webpages
Frequently Asked Questions

Q1: What has changed?
A: The safety of your participants' personal information is a top priority at Fidelity, and we are implementing new security protocols to add another layer of protection to your participants' accounts. Today, third-party financial data aggregators can access certain information through specific webpages on NetBenefits and our other websites (i.e., Fidelity.com, Wealthscape Investor) when participants give their Fidelity credentials. In the future, these third parties will access data through secure applications provided by Fidelity. Due to technology changes, financial data aggregators may experience additional multi-factor authentication prompts as well. We are making these changes with your participants' best interests in mind to reduce the amount of participant data these third parties have access to.

Q2: How will this change impact participants?
A: We are working with third-party sites and applications to make their access to Fidelity websites, including NetBenefits, more secure. After these enhancements are implemented, depending on which third-party sites or apps a participant uses, participants may temporarily be unable to access some of their Fidelity data on that site. It does not mean the information is lost or compromised in any way, and participants can still access all their data on NetBenefits, Wealthscape Investor, Fidelity.com and our mobile app. Your participants expect Fidelity to provide world-class data protection, and this is another example of us delivering on those expectations.

Q3: Can you tell me more about third-party data providers?
A: Third-party data providers serve as financial aggregator platforms and facilitate data exchange between authorized businesses. Typically, consumers use these services to pull together information from multiple financial platforms into one view. Examples include Intuit/Mint, Envestnet/Yodlee, Finicity and Plaid. To use these services, consumers are typically required to share usernames and passwords, which we do not believe is in line with evolving cybersecurity or data protection best practices.

Q4: Why is Fidelity concerned about current data aggregation practices?
A: Third-party financial applications typically require users to share usernames and passwords for financial accounts they hold elsewhere and then they use that information to access those accounts and extract account data.

Once consumers grant access to third parties, including data aggregators and fintechs, these firms typically employ bots to login to financial accounts on behalf of the consumer and access all available information.

While we support consumers' right to grant access to data from their financial accounts to outside service providers, we feel strongly that they should be able to do so without having to share their usernames and passwords.

Q5: What is multi-factor authentication (MFA) and how is it different from two-factor authentication (2FA)?
A: Multi-factor authentication is an authentication method that requires two or more verification factors to gain access to a platform. Multi-factor authentication enhances security and reduces sensitive participant data exposure. Two-factor authentication is a method that requires only two verification factors. *(See below for more detailed information.)*

Q6: What are the benefits of allowing aggregators access to information through specific webpages or secure applications, and prompting them with multi-factor authentication?
A: The safety of your participants' personal information is a top priority at Fidelity and these changes allow us to better control the flow and access to information by enhancing security and reducing sensitive participant data exposure.

Q7: Which third-party providers are impacted by this change?
A: Any financial aggregator could be impacted, including Envestnet/Yodlee, Intuit/Mint, Finicity, Plaid and associated providers such as Venmo.

Q8: When did this change go into effect?
A: This change will be in effect early December 2022.

Q9: Did Fidelity take this action in response to a cyber incident or data breach involving financial aggregators?
A: No, this was not a result of any cyber incident, data breach or loss of participant information. The safety of your participants' personal information is a top priority at Fidelity. This action was taken to further enhance security and reduce the risk of potential data breaches or exposure. Fidelity regularly reviews and updates its security measures.

Q10: What if a financial provider can no longer access a Fidelity customer's account information?
A: If this situation occurs, we will ask the participant for the name of the provider and let them know that we will share this information with the appropriate teams for review. In the meantime, the participant is welcome to follow up with their provider directly to understand if they are working with Fidelity. Our goal is to work with the financial aggregation platforms to exchange certain information securely.

Participants can take steps to protect their information and data, including:

- Confirming whether they still actively use all the sites and apps that have their Fidelity username and password.
- Determining whether they want to continue sharing their Fidelity access with these sites.

- Reading the terms and conditions of sites that have their login credentials, to ensure they know how the data is used and stored, whether they sell any of the information, and what happens to the data if they leave the service, or if the service doesn't exist anymore.
- Setting up alerts to stay informed on their account activity.
- Monitoring their accounts regularly for any unusual activity.

Q11: How does this change impact Fidelity's Full View?
A: Participants who use Full View on Fidelity.com and NetBenefits.com will not be impacted, as Fidelity information is accessed through a secure application (API). However, investors who work with an independent advisor using the eMoney Advisor planning tool and who have accounts with Fidelity will likely be impacted, as eMoney will only be able to access information through specific webpages or secure applications and be prompted with multi-factor authentication.

Q12: Will the healthcare data for health savings accounts (HSAs) be impacted?
A: This change will not impact the healthcare data for HSAs.

Q13: How will this change impact participants who use TurboTax?
A: This change will not impact the use of TurboTax for participants.

Q14: What if a participant wants an impacted third-party provider to have their data?
A: Participants can manually enter data on the third-party provider's website.

Q15: Can plan sponsors opt out of this change? Why not?
A: No, the use of a third-party data provider is something an individual chooses on their own to help them meet their personal financial needs and goals. Furthermore, a plan sponsor cannot limit an individual's use of their own information.

Q16: Will participants ever be able to use an impacted third-party site to access their Fidelity information again?
A: That is certainly our intent. We are working with these sites to allow participants to access their Fidelity information when and where is convenient for them—but only while ensuring these access points meet our own high standards of security.

Any interruptions in service should be temporary while we implement the new security protocols. We apologize to participants if they experience any interruption to sharing their Fidelity account data with third-party websites or apps.

Q17: Does a participant have to take any action at this time to continue to conduct business with Fidelity?
A: No. Participants can continue to view, access, and manage all accounts on NetBenefits, Wealthscape Investor, Fidelity.com or within the Fidelity mobile app.

Q18: Can a participant turn screen scraping off?

A: Yes, participants can change their Fidelity password to prevent third-party apps and websites from collecting their data or remove their account information from those providers.

Q19: Can a plan sponsor turn screen scraping off for their organization/company?
A: No, a plan sponsor cannot turn screen scraping off for their participants' accounts.

Q20: What steps can a participant take to protect their information and data?
A: Participants can take steps to protect their information and data, including:

- Confirming whether they still actively use all the sites and apps that have their Fidelity username and password.
- Determining whether they want to continue sharing their Fidelity access with these sites.
- Reading the terms and conditions of sites that have their login credentials to ensure they know how the data is used and stored, whether they sell any of the information, and what happens to the data if they leave the service or if the service doesn't exist anymore.
- Setting up alerts to stay informed on their account activity.
- Monitoring their accounts regularly for any unusual activity.

Q21: What additional security does Fidelity have?
A: Fidelity has a range of safeguards and multiple layers of security in place to protect participant accounts and information, our sites, and systems. For security purposes, some are visible and some are not.

Multi-Factor Authentication (MFA)

Q22: What is Multi-Factor Authentication (MFA) and what is the value of being enrolled in MFA?
A: With multi-factor authentication, an extra layer of security is added to an account to prevent someone from logging in, even if they have the account password. This extra security measure, which, for example, can be a text or a phone call, requires a participant to verify their identity using their password and a second level of verification to help prevent unauthorized access.

Q23: What is the benefit of Multi-Factor Authentication?
A: The safety of your participants' personal information is a top priority at Fidelity, and with an increase in the risk of password and identity thefts through tactics such as phishing, MFA is critical as we continue to protect participant data. This next-level security layer reduces identity and fraud risks by making it harder for cyber criminals to get access to accounts and personal information.

We continuously look to improve the participant experience while also ensuring the security of their data.

Q24: Is the existing MFA experience improving?
A: We have heard from your participants that they want more authentication options, and we will roll out more options throughout 2023 – such as push notifications, third-party authenticators, and security keys -- to improve your participants' experience. As third-party data providers update their sites to work with our MFA solutions and move to our APIs, the user experience will also improve.

Q25: Why does Fidelity limit MFA to Symantec VIP or SMS?
A: In the coming year, we will begin offering more options to enhance security and your participants' experience, such as push notifications, third-party authenticators, and security keys.

Q26: What transactions are protected?
A: Certain high-risk transactions are protected with auto-enrolled MFA.

In addition to the security provided through MFA, which secures a participant's account even if a password has been compromised, all transactions are covered by the Customer Protection Guarantee. This means that Fidelity will reimburse participants for losses from unauthorized activity in covered accounts occurring through no fault of their own. The Customer Protection Guarantee does not apply if a participant shares their username and password with a third party.

# # #

Fidelity Brokerage Services LLC, Member NYSE, SIPC,
900 Salem Street, Smithfield, RI 02917