PRESENTED BY: DAVID SCHNEIER– FIDELITY CUSTOMER PROTECTION

Protecting what matters:

Our customers' trust and financial future

Fidelity INVESTMENTS

DOL Issues Guidance on Cybersecurity, April 2021

Three focus areas for plan sponsors, recordkeepers, and participants

Plan sponsors

Designed to assist plan sponsors fiduciaries in their evaluation of the cybersecurity practices of service providers.

View guidance

Cybersecurity Best Practices

Best practices for recordkeepers and other service providers outlining key elements of a cybersecurity program.

View guidance

Online Security Tips for Retirement Investors

A series of recommendations for plan participants to prevent fraud and loss of access to a retirement account.

View guidance

When participants are victims of fraud, plan sponsors may be responsible

Fraud

Recordkeeper, Plan Sponsor Charged in 401(k) Account Theft

Alleged fraud drains retiree's 401(k)

Plan's administrator facing federal probe into unauthorized distributions

Lawmakers Ask GAO to Examine Cybersecurity of Retirement System

What are you doing to ensure the security of your employees' accounts?

Fidelity is committed to protecting our customers

We keep your data and employees safe with significant investments in cybersecurity

We protect and treat your data as if it were ours

Comprehensive controls, processes, and systems in place to help ensure your data is safe, secure, and private

We employ National Institute of Standards and Technology (NIST) Cybersecurity Framework

Guidelines to **create**, **guide**, **assess,** or **improve** comprehensive cybersecurity programs

International certifications and Independent audits

ISO 27001 & ISO 27017 (NEW)
Data security and cloud security

ISO 27701
Data privacy

ISO 22301
Business resiliency

SOC 2 Report Type II

We protect your greatest asset: your employees

An industry-leading[1] customer protection program focusing on protecting individual customers from account compromise, fraud, and identity theft

Proprietary fraud detection and prevention

Anomalous activity and pattern recognition utilizing internal and external intelligence

Compromised credential testing

In the last 5 years, **1,300,000+ Fidelity accounts have been proactively blocked[2]**

Account protection features

Two-factor authentication

Real-time alerts for high-risk transactions

MyVoice® phone authentication

59% of calls are authenticated with MyVoice[2]

Click to view demo

Fidelity's Customer Protection Guarantee

Participants reimbursed for losses from unauthorized activity through no fault of their own, with no dollar limit

Click to view guarantee

[1] In the "2020 User Authentication and Security Assessment" study conducted by Corporate Insight, Fidelity stands out among banks and brokerages for imposing a 2FA step for profile updates and money movement transactions on the website and app, and is the only firm among banks and brokerages that allows clients with different account types to enhance the security of login recovery process with a soft token.

[2] Fidelity Investments data as of January 2022

Protecting what matters: Our customers' trust and financial future

You can be confident that your organization is protected with Fidelity's industry-leading cybersecurity