Nationwide®
is on your side

Committed to cybersecurity and fraud prevention

We take safeguarding participant data and assets seriously

Near-daily headlines confirm that cyberattacks and cyberfraud have become all too common. In fact, there were 4.8 million identity theft and fraud complaints filed with the Federal Trade Commission in 2020 alone.[1] Many of the old scams have been modified to take advantage of the COVID-19 pandemic.

Criminals tend to go where the money is. With more than $37.4 trillion invested in retirement assets as of Sept. 30, 2021,[2] participant accounts make attractive targets for criminals. At Nationwide®, we relentlessly focus on plan security and protecting participants' data, privacy and assets.

Focused protection against cyberthreats and fraud

Our holistic approach to security and protection layers people, processes and technology to help keep your plan and participant data safe. Over the next few pages, we discuss recent U.S. Department of Labor guidance on retirement plan cybersecurity. Then we explain how Nationwide's cybersecurity practices meet the recommendations outlined by the DOL guidance. Finally, we explore how Nationwide uses technology and training to help combat fraud before it gets started and arrest it before it can spread.

Cybersecurity

Protection of computer systems from the theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services provided

VS

Fraud

Deceptive practices resulting in financial or other losses for consumers/companies in the course of seemingly legitimate business transactions

All the defenses in the world cannot protect from theft when common sense and caution are ignored. As you review this document, consider how you and your participants can help protect yourselves from those who seek to use times of crisis for their own benefit.

DOL cybersecurity guidance

Recently, the Department of Labor issued new guidance on retirement plan cybersecurity. Focusing on three key areas of best practices, this guidance offers a checklist to consider when reviewing your or your partners' approach to cybersecurity and data protection.

Training and best practices

- Clearly define and assign information security roles and responsibilities
- Have strong access-control procedures
- Ensure that any assets or data stored in the cloud or managed by a third-party service provider are subject to appropriate security reviews and independent security assessments
- Conduct cybersecurity awareness training at least annually and update training annually to reflect risks identified by the most-recent risk assessment

Security assessment

- Have a formal, well-documented cybersecurity program
- Conduct prudent annual risk assessments
- Have a reliable annual third-party audit of security controls

Data security and encryption

- Implement and manage a secure system development life cycle (SDLC) program
- Have an effective business resiliency program addressing business continuity, disaster recovery and incident response
- Encrypt and protect sensitive data and nonpublic information both in transit and at rest
- Implement strong technical controls in accordance with best security practices
- Take appropriate action to protect the plan and its participants when a cybersecurity incident or breach occurs

People and processes power our cybersecurity and fraud prevention defenses

Fraudsters and cybercriminals rely on humans to be human. They exploit human vulnerabilities, which is why our first layer of defense starts with our people.

200 information risk professionals

Our professionals devote each day to thinking about how to better protect participant data.

- They conduct attack and penetration testing to help ensure that our data is secure.
- They help ensure that our software is up to date to prevent intrusion
- They help ensure that we use secure tools such as multifactor authentication to ensure that access is being granted through trusted devices

Associate training

Everyone who has access to plan and participant information receives detailed training on how to be aware of security and fraud threats as well as techniques that can help them be continually diligent for these threats.

In addition, each Nationwide associate:

- Completes annual security and fraud education. A portion of this training is focused on phishing — how to identify it and what to do if phishing is detected.
- Is tested with targeted emails throughout the year. Failure requires additional training.
- Receives training on fraud prevention, focusing on how to identify fraud and what to do if they suspect it.

Knowing what specific actions to take

Our fraud detection processes are rigorous and focused on assuring that we are dealing with the real participant and legitimate transactions. By following a clearly defined, monitored and quality-controlled process, we help protect participants from fraudulent distribution attempts.

This process includes:

- Stepped-up validation of participants when they call our Solutions Centers
- Thorough review of distribution requests for critical fraud red flags
- Extra validation steps if there are concerns or red flags with call or distribution requests

We employ the same thorough security steps no matter whether the person is requesting service over the phone, on paper or over the internet.

Proactive distribution alerts

When we process a distribution, we send a communication to the participant to let them know that we processed their distribution. If the distribution would happen to be fraudulent, this alerts the participant that something is wrong so they can contact us and can also lock down other financial accounts they might have elsewhere.

Technology helps keep out bad actors

Nationwide employs powerful weapons to protect participants from being defrauded.

Phoneprinting™ technology analyzes each call, using more then 1,000 attributes that look at things like device, behavior and voice to help determine whether it is potentially risky or fraudulent, so our associates can take additional steps to ensure that the account remains well-protected.

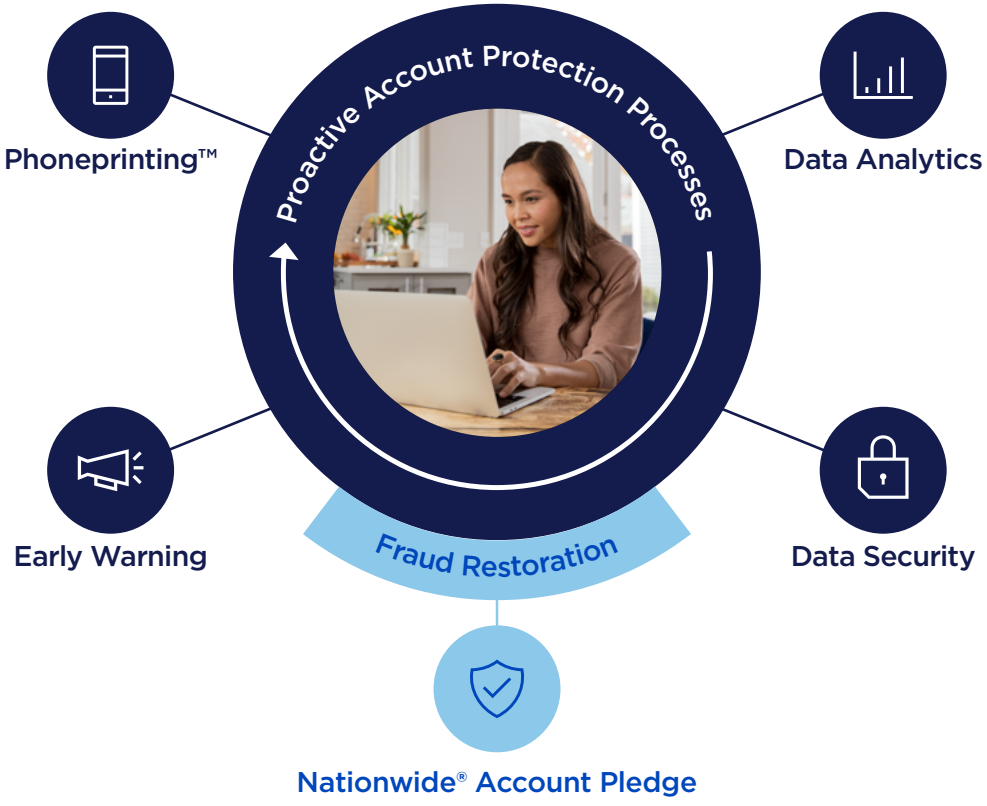
Early Warning technology allows us to collaborate with banks to complete various validations before we process the transaction. This technology helps ensure distributions are being sent to the participant.

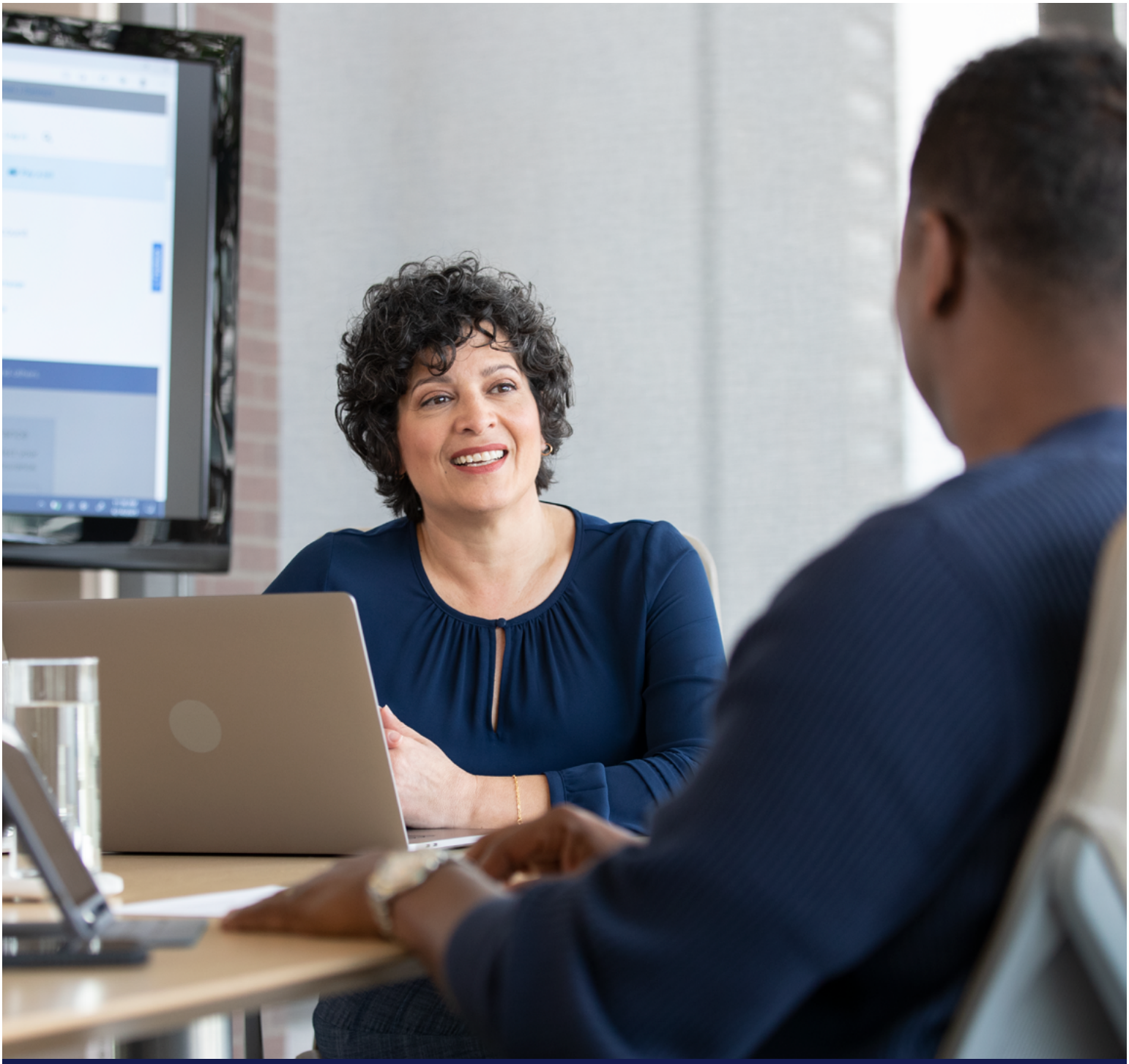
Nationwide Account Pledge is our commitment to protect participants if fraud happens.[3] For more information about our pledge, visit nationwidefinancial.com/accountpledge.

We focus on fraud prevention, server safeguards, and secured files, building and networks.

Our analytics are designed to identify potential fraud and wall it off when possible.

Fraud protection





Industry partnerships

We partner with the Financial Services Information Sharing and Analysis Center and other industry partners to understand threats and improve our perimeter.

Nationwide remains committed to investing in its people, processes and technology to enhance its already strong cybersecurity program and to deliver better experiences, while also vigilantly defending the retirement benefits and personal information with which we have been entrusted.

To learn more, contact your Nationwide representative or call **1-800-626-3112**.

Nationwide®
is on your side

[1] "Consumer Sentinel Network Data Book 2020," Federal Trade Commission (revised Sept. 30, 2021).

[2] "Retirement Assets Total $37.4 Trillion in Third Quarter 2021," Investment Company Institute (Dec. 16, 2021).

[3] Nationwide Account Pledge is subject to certain limitations and restrictions.

The information presented is intended for educational purposes only and is not meant to be all-inclusive for all factors related to fraud and cybersecurity. It is not intended to be a substitute for professional advice, legal or otherwise. If you have questions regarding which anti-fraud prevention techniques may be most effective for you, please check with your own legal counsel or cybersecurity professional.

The Financial Services Information Sharing and Analysis Center is not related to or affiliated with Nationwide or any of its affiliates.

FOR FINANCIAL PROFESSIONAL, ADMINISTRATOR AND PLAN SPONSOR USE — NOT FOR DISTRIBUTION TO THE PUBLIC

PNM-19457AO.1 (04/22)