PSERS
PUBLIC SCHOOL EMPLOYEES' RETIREMENT SYSTEM

Keeping your accounts secure

It's important to safeguard your financial accounts and personal information against the ongoing risk of fraud, cyber threats, and other unauthorized activity. You should treat your account numbers, PINs, passwords, and personal information as the keys to your accounts.

We believe that keeping your account secure is a mutual responsibility. As a result, we recommend you take action to protect your accounts and identity. One of the most critical and easiest steps you can take to keep your accounts safe is to register them online. If you have not registered your PSERS accounts online, you are at a greater risk of having your accounts compromised. Fraudsters, for example, like to target unregistered accounts that they can set up with their own data points like phone number and email address. You are more secure by registering your accounts online.

Register your PSERS Member Self-Service (MSS) account online and access your PSERS DC account

The first step you should take is to complete the registration for your PSERS MSS account. Visit ***psers.pa.gov*** and click *Member Login (MSS)*. You will have to provide your PSERS ID, social security number, and date of birth to register and create an account username and password. Through your MSS home page, click the link in the *Voya Account Access* box to access your PSERS DC account.

Here are some additional suggestions to consider to help you keep all of your personal accounts (including your PSERS DC Account) and personal information safe and secure:

General Password/PIN Security

- Use a unique password/PIN for each site where you maintain an account and regularly update your passwords/PINs. Never use your date of birth or social security number as your password/PIN.
- The strongest passwords are comprised of a chain of four unrelated common words.
- Don't allow social networking sites to memorize your passwords/PINs.
- Avoid writing down passwords/PINs.
- Don't share your password/PIN or answers to security questions with anyone and never put them in an email.

Beware of "Phishing"

A phishing attack is an online fraud technique that involves sending official-looking email messages with return addresses and links that appear to originate from legitimate businesses, often times with corporate branding. These emails typically contain a hyperlink to a spoof website. It is important to be suspicious of emails asking for your confidential information and look out for red flags such as urgent requests, unknown email addresses, or discrepancies between actual and displayed hyperlinks. Neither PSERS nor Voya will ever ask you for your personal information by email.

Monitor your accounts frequently

- Monitor your financial accounts frequently, and be sure to look for unusual withdrawals, deposits, or transactions. The PSERS MSS Portal and your PSERS DC account make monitoring easy.
- Sign up for electronic delivery of important documents. Go to your PSERS DC account and click *My Profile > Communication Preference*s to sign up.
- Immediately open your statements and emails regarding your account. Monitor and confirm all activity. If you notice anything suspicious, call your financial institution immediately.

92779-0085-I

Take care of your computer and mobile devices

- Update your computer by installing the latest software and patches to prevent hackers or viruses from exploiting any known weaknesses on your computer.
- Install and update anti-virus software to protect your computer and to prevent hackers from installing malware or viruses on your computer.
- Install and update personal firewalls. A firewall is a hardware or software device that regulates the flow of information between computers and is often included in operating systems.
- Use only programs from a known, trusted source.
- Backup your important files on a regular basis and store the backups in a secure place.

How Voya® is keeping your PSERS DC account safe

Voya takes numerous measures to safeguard the confidentiality, integrity, and availability of their systems, including authentication, monitoring, auditing, and encryption. Voya is constantly evolving their strategies to address and adapt to anticipated threats.

If you suspect fraud on your PSERS DC account, Voya will investigate the incident to determine the best course of action, which may include free credit monitoring or identify theft protection and possible reimbursement of financial loss.

Voya S.A.F.E.® (Secure Accounts for Everyone) Guarantee

If any assets are taken from your PSERS DC account due to unauthorized activity and through no fault of your own, we will restore the value of your account. To help prevent this from occurring and to comply with the S.A.F.E Guarantee's requirements, you have the responsibility to:

1. Register your PSERS MSS account online.
2. Review your account information on a regular basis and keep your contact information current.
3. Promptly report any suspected identity theft or unauthorized activity.
4. Contact Voya at *1.833.432.6627 (1.833.4DC.MMBR)* if you receive a PSERS DC account alert that you did not initiate.
5. Practice safe computing habits.

Secure your accounts today

Remember that you are your own first line of defense when it comes to protecting your accounts and identity. Keep your accounts and personal information safe and secure. Visit ***psers.pa.gov*** to get started.

PSERS®
PUBLIC SCHOOL EMPLOYEES' RETIREMENT SYSTEM

With PSERS, you're on your way!