PUBLIC SCHOOL EMPLOYEES' RETIREMENT SYSTEM

SPECIAL REPORT

Identity theft

Whose name is it anyway?

A man walks up to a bank teller, provides his name, address, mother's maiden name and social security number – and opens a new bank account. The only problem: the information he provided was yours. And now he has a credit card with your name. Your identity has been stolen. Could this have been avoided?

This information is provided by the Voya family of companies for financial education and awareness purposes to all PSERS members and participants in PSERS Class T-G, Class T-H, and Class DC and does not constitute financial advice.

A case of stolen identity

Someone stealing your identity and passing as you may sound like a movie plot, but for millions of Americans each year, it's not a screenplay. It's a nightmare that costs significant time and money to fix.

But by taking the right steps, you can help protect yourself.

Your information is at risk

You're probably familiar with identity theft in its simplest form: someone uses your credit card to fraudulently purchase items. But identity thieves can take advantage of your personal information in much more sophisticated ways.

Your head and wallet are full of information you use every day: credit card and bank account numbers, PINs, date of birth, mother's maiden name, home address, and your employer information. Perhaps the most important of this information, though, is your social security number. When combined with other personal information, it can allow identity thieves to:

- Access your checking or savings account.
- Change your bank account passwords.
- Open a new account in your name.
- Establish a new identity for someone to help obtain a job or driver's license.

Stop! Thief!

Some common ways identity thieves use to steal personal information include:

- **Mail Theft** – Someone steals your utility bill from your mailbox and uses the information to respond to a pre-approved credit card offer.
- **Shoulder Surfing** – Someone overhears you say your account number and mother's maiden name while talking to your bank on your cell phone in public.
- **Solicitation** – You respond to a telephone survey and inadvertently provide personal information about your bank account.
- **Dumpster Diving** – Someone goes through your trash and finds your old cancelled checks, which may include your bank account number, address, phone number, and social security number.
- **Hacking** – Someone gains illegal access to your employer's database, which includes your social security number, address, phone number, and checking account number.
- **Phishing** – You respond to a phony email asking you to update your personal banking information and inadvertently send your information directly to a scammer.
- **Pharming** – You accidentally type an incorrect (but similar) website address – such as charity.com instead of charity.org – and make an online donation to a scammer who has set up a site to catch poor typists.
- **Inside Access** – You fill out an application for a car loan and an unscrupulous employee at the dealership helps himself to your personal information.

Protect yourself

To avoid having your identity stolen, take the following actions:

- **Guard your info** – Lock up your personal financial data and your passport, shred credit offers and financial documents, and take outgoing mail to a U.S. postbox.
- **Change risky habits** – Don't carry your social security card in your wallet, write PINs on your cards or keep financial documents in your car's glove box. Avoid choosing obvious passwords.
- **Use good computer sense** – Install anti-virus/spyware on your computer. Be sure not to store personal data on your laptop, click suspicious links or respond to an unsolicited email. Call your financial institution if you doubt an email's authenticity.
- **Take public precautions** – Take credit card receipts with you and never announce your social security number or personal data in public.
- **Be proactive** – Review your financial statements each month, get a free credit report once a year, monitor your checking account activity, and always question why someone needs your social security number.

Theft happens

Despite your best efforts, identity theft can still happen. If someone steals your personal information, you should notify the following organizations:

- **Federal Trade Commission** – Go to *consumer.gov/idtheft* and file a complaint.
- **Credit bureaus** – File a fraud alert in writing with one of the three major credit reporting agencies: Experian, TransUnion, or Equifax. Instructions can be found on their websites.
- **Your creditors** – Contact all financial institutions where affected accounts are held and request in writing that a hold be placed on the account.
- **Police** – File a police report, which is required for most claims on identity theft.

Note that if your social security number is stolen, be sure to contact all financial institutions and creditors affected. The Social Security Administration (*ssa.gov*) can also provide additional assistance.

Name damage

The aggravation of identity theft goes beyond the cost in dollars, as victims can spend months resolving the issue. But even worse is the long-term damage it can do to your name by affecting your credit rating. A bad credit rating can affect your ability to obtain a loan or increase your insurance rates. By guarding your personal information, you can help avoid these scenarios.

With PSERS, you're on your way!

PSERS®
PUBLIC SCHOOL EMPLOYEES' RETIREMENT SYSTEM