MainePERSpective

Retiree Edition
Winter 2026



Message from the CEO

This issue of the ***MainePERSpective Retiree Edition*** provides important tax updates to keep in mind as you prepare your 2026 income tax filing. With the increase in online scams, a special Online Security and Fraud Prevention Section is included with information about some of the common fraudulent tactics and scenarios being used and how to respond in these situations.

Additionally, the enclosed 2027 calendar highlights the dates your benefit payments will be direct deposited into your account.

We wish you an enjoyable Holiday season and a Happy and Healthy New Year!

Best regards,

Dr. Rebecca M. Wyke
Chief Executive Officer

Annual Notice of Right to Elect or Revoke Federal Tax Withholding

You have the right to decide whether you want federal income tax withheld from your monthly MainePERS benefit payment. When making your decision, remember that you are still responsible for payment of federal income tax on the taxable portion of your MainePERS benefit when you file your tax return. Not having enough tax withheld or paid during the year could leave you subject to tax penalties. You may change your current withholding election by sending us a completed *W-4P, Withholding Certificate for Periodic Pension or Annuity Payments*, which you can find on the Internal Revenue Service website at www.irs.gov or at www.mainepers.org/forms/retiree-forms/. No action is necessary if you do not wish to change your current federal income tax withholding.

Download your *1099-R* Form from the MainePERS Member Portal

In January of each year, MainePERS mails an Internal Revenue Service Form *1099-R* to each person who received either a benefit payment or a refund of contributions in the prior calendar year.

In late January 2027, the form also may be accessed through the MainePERS Member Portal. You can locate your Form *1099-R* by clicking on the Documents Tab and easily view the information or download the form.

If you have not registered for the Member Portal you may register at www.mainepers.org/memberportal. A handy guide is available to help with the process.

By February 15, 2027, if you have not received your *1099-R* in the mail and do not have access to a computer and printer, please contact MainePERS at 207-512-3100 to request a duplicate copy.

BOARD OF TRUSTEES
Brian H. Noyes, *Chair*
Richard T. Metivier, *Vice Chair*
John S. Beliveau
Shirrin L. Blaisdell
Kirk Duplessis
Nick Fuller Googins
John H. Kimball

Ex-Officio Member
Joseph C. Perry, State Treasurer

CHIEF EXECUTIVE OFFICER
Dr. Rebecca M. Wyke

RETIREMENT SERVICES
(207) 512-3158

EMPLOYER SERVICES
(207) 512-3200

GROUP LIFE INSURANCE
(207) 512-3244

DISABILITY SERVICES
(207) 512-3170

Mailing Address
P.O. Box 349
Augusta, ME 04332-0349

Location
139 Capitol Street, Augusta, ME

Phone
Main: (207) 512-3100
Toll-Free: 1-800-451-9800
Fax: (207) 512-3101
Maine Relay: 711

Public Business Hours

The MainePERS lobby is open Monday through Thursday from 8:00 a.m. to 4:00 p.m.

Member Services Representatives are available to assist you by telephone, email and in person Monday through Thursday from 8:00 a.m. to 4:00 p.m.

MainePERSpective

Published by
Maine Public Employees Retirement System (MainePERS).

A printed version of the ***MainePERSpective - Retiree Edition*** newsletter is mailed out to retirees. We also email an electronic copy to retirees who have a current email on file with us. We hope to provide retirees with the option of selecting their preferred mode in the near future.

Maine Income Tax and Pension Income Deduction

Individuals who receive MainePERS benefits and file their taxes in the State of Maine may qualify for a pension income deduction for all or part of their MainePERS benefit. The amount of the pension income deduction available is based on the maximum annual Social Security benefit for someone retiring that year at full retirement age reduced by any Social Security or railroad retirement benefits received.

For individual taxpayers, the maximum deduction for tax year 2026 is $49,824. This deduction begins phasing out at adjusted gross incomes greater than $125,000 for single tax return filers, $187,500 for head-of-household filers, and $250,000 for joint filers.

Please note, a new Form *W-4ME* must be filed with MainePERS if you would like to change your state withholding. This form may be found at www.mainepers.org/forms/retiree-forms/. If you have a tax preparer or advisor, they should be able to address any questions about the Maine pension income deduction. Questions also may be directed to Maine Revenue Services at 207-626-8475.

Gross Income Exclusion for Eligible Retired Public Safety Workers

Are you a retired public safety worker receiving your pension from MainePERS? Did you retire at or after your normal retirement age, or due to disability?

If you answered yes to both of these questions, you may be able to exclude up to $3,000 from your gross taxable income for health insurance dollars you paid. Health insurance premiums deducted from your MainePERS benefit or paid directly by you to the insurer can qualify.

For more information, please see *IRS Publication 575* or contact a tax preparer or advisor.

Estate Planning and Your Beneficiaries

Losing a loved one is difficult, and navigating estate details can be confusing. Whether you are a beneficiary or retiree, consider including information about notifying MainePERS of your passing as part of your estate planning instructions. This will begin the process of ensuring proper distribution of any pension or group life insurance benefit to your intended beneficiaries.



An online form is available to help begin the process and can be accessed from the MainePERS homepage www.mainepers.org (look for the "*Notification of Death*" button). Notification also may be made via telephone, 207-512-3100, or email survivor.services@mainepers.org.

Special Online Security and Fraud Protection



Imposter Scams – What to look for and how to prevent them

Recent headlines provide heartbreaking stories of individuals who have had their retirement savings stolen by bad actors:

"Elderly couple in Gray recovers $19,500 from online fraud," *Portland Press Herald*, November 9, 2025
www.pressherald.com/2025/11/09/elderly-couple-in-gray-recovers-19500-from-online-fraud/

"How a Maine couple gave their $1.3 million retirement savings to bitcoin scammers," *Portland Press Herald*, November 20, 2025
www.pressherald.com/2025/11/20/how-a-maine-couple-gave-their-1-3-million-retirement-savings-to-bitcoin-scammers/

The Federal Trade Commission (FTC) has outlined some scenarios used by scammers to gain the trust of their victims and ways individuals can protect themselves. Below are excerpts from "*False alarm, real scam: how scammers are stealing older adults' life savings*"* an August 7, 2025, article from the FTC Division of Consumer Response and Operations.

"Reports to the FTC show a growing wave of scams aimed squarely at retirees' life savings. These scammers pretend to be from known and trusted government agencies and businesses.

These high-loss scams typically start with a (fake) story that gets your attention with one or a combination of these lies:

- **Lie #1:** Someone is using your accounts. This lie might start with someone pretending to be your bank, flagging so-called suspicious activity, or pretending to be a well-known national online retailer with a message about an unauthorized purchase;
- **Lie #2:** Your information is being used to commit crimes. This lie may come from a supposed government officer or agent, warning that your Social Security number is linked to a crime like drug smuggling, money laundering, or even child pornography; or
- **Lie #3:** There's a security problem with your computer. This lie often starts with a fake on-screen security alert that looks like it's from Microsoft or Apple with a number to call. If you call, they say your online accounts have been hacked.

These scammers say the only way out of the (fake) crisis is to follow their instructions – which will include sending money to the scammers. They may say this will keep your money safe, secure your identity, clear your name, or help catch the criminals. There may be layers of complexity to the story, but it's all a lie aimed at draining your accounts. Reports show that when people think they are fixing a problem rather than sending a stranger money, their losses are often limited only by their available funds.

The security of your accounts, along with the risk of identity theft, are real concerns that real companies might call you about. So how can you stay vigilant and steer clear of these scams?

- **Don't move money to "protect it."** Never transfer or send money to anyone, no matter who they say they are, in response to an unexpected call or message. Even if they say it's to "protect it."
- **Hang up and verify.** Hang up the phone and call the company or agency directly using a phone number or website you know is real. Don't trust what an unexpected caller says, and never use the phone number in a computer security pop-up or an unexpected text or email.
- **Block unwanted calls.** Learn about your call blocking options to stop many of these scammers before they reach you."

Additional FTC online resources:

- **How to learn more about imposter scams** - https://consumer.ftc.gov/features/how-avoid-imposter-scams
- **How to activate call blocking options** - https://consumer.ftc.gov/articles/how-block-unwanted-calls
- **How to spot and avoid scams – and learn how to recover money if you paid a scammer** - consumer.ftc.gov/scams
- **How to report scams to the FTC** - reportfraud.ftc.gov

**The complete FTC article may be found at www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/08/false-alarm-real-scam-how-scammers-are-stealing-older-adults-life-savings*

(continued on page 4)

Special Online Security and Fraud Protection (continued from page 3)



Online banking security measures

Online apps and interactions can make life easier, and these innovations have provided greater access to many services. This includes online financial apps or online banking and the rising popularity of completely digital branchless financial institutions, also known as neobanks.

Neobanks offer banking services through digital means only. There is no brick-and-mortar branch location to visit and interact with someone face-to-face. All transactions and communications take place electronically through telephone, email, and online or mobile applications. The use of these completely digital financial services is growing and while they may provide many benefits, some cybersecurity risks, such as identity theft and account takeovers, may be heightened by the completely digital nature of the banking relationship. To guard against these risks, users of branchless banking should be vigilant in asking about cybersecurity protections, including the use of **user identification verification** and **multifactor authentication**, before depositing funds, and once an account is established, monitoring their online accounts and credit reports, as a regular financial wellness activity.

User Identification Verification Process
Simply put, this is the process a bank uses to be sure that you are who you say you are. A neobank should take the same precautions that a brick-and-mortar bank does when opening an online account. If you are not required to provide some form of identification as part of opening your completely online bank account, ask more about the bank's security policies or consider finding another online financial institution.

Multifactor Authentication
Be sure your financial institution provides multifactor authentication (MFA), also sometimes referred to as two-factor authentication. This protection is multifactor because it requires two separate ways to authenticate that YOU are the person trying to access YOUR account.

The first authentication is your password. The second authentication is usually a unique one-time security code number sent to you through a text, email, or in some instances telephone voice message to confirm access should be permitted. (The way you receive it is prearranged by you with the institution.) While a bad actor might have obtained inappropriate access to your password, in most instances the bad actor would not have access to the unique one-time code sent directly to you. Without the security code, access to your account will be denied.

Whether you choose the completely online services of a neobank or decide to use a traditional brick-and-mortar financial institution that offers online services, be sure security features are in place to safeguard you and your money. Not all institutions provide the same level of protection, so it is important to check.

And a final word about secure passwords

The first line of defense in any online activity is creating a secure password and **changing it on a regular basis**. Some additional tips to keep in mind regarding passwords:

- Use a combination of upper-and lower-case letters, numbers, and symbols.
- For extra security, use longer passwords.
- Never use personal information in your password.
- Do not use the same password for multiple accounts or sites.
- Random passwords are the strongest (those that do not contain a set pattern or common words).

Finally, consider a password manager to generate a random password and also keep track of all your passwords. This provides added security by eliminating the need to write down your passwords where someone could find them. Several commercial password managers are available for use with your computer, cellphone, and other electronic devices.