Dear Participant,

For the past three weeks, we've written about ways criminals trick individuals into sharing private information. It's a good idea to stay aware of scams to protect yourself—but what if your information is already compromised? And how do you know if it is compromised? We will provide some clues offered by the Federal Trade Commission to determine if someone has used your information fraudulently as well as steps to take once you know.

At Wespath, we are committed to providing secure access to your retirement account and investment information. On June 6, we'll unveil enhancements to our participant account management website, Benefits Access. As announced last week, the updated site will be easier for you to view on your smartphone or tablet and will offer more intuitive navigation. Read on for your first look at the new site.

While Benefits Access is designed to support your financial well-being, Wespath also supports the health of our participants in all dimensions—spiritual, emotional, physical, social and financial. Our next issue of the *Dimensions* newsletter will feature insights from participants who have taken a personal or professional sabbatical or formational leave of several weeks to months to improve their well-being. If you would like your story to be considered, contact us at wellnessteam@wespath.org.

For the most current information about Wespath's COVID-19 response, please go to Wespath's Coronavirus webpage or follow Wespath on Facebook and Twitter.

How to Recover When Your Personal Information has Been Stolen

Last year, a research study found that 14.4 million people were victims of identity fraud. Thieves can do much more than make purchases with your stolen financial data. The Federal Trade Commission (FTC) reports identity theft can also drain your bank accounts, open new utility accounts, get medical treatment on your health insurance, file tax returns in your name and receive your tax refund, cause you trouble with police by providing your name during an arrest and even resell your information to other criminals.

It's important to act fast, since delays in identifying a data compromise can allow thieves to do more damage to your financial future. So how do you know if criminals have stolen your personal information?

Clues That Your Information Has Been Stolen
According to the FTC, you should look out for the following clues:

- You see bank withdrawals you didn't initiate or unknown charges on your credit card
- You don't receive bills or other mail you were expecting
- Your checks are refused
- You receive calls from debt collectors about debts that aren't yours
- Your credit report shows unfamiliar accounts or charges

- You receive medical bills for services you didn't use
- Your medical records show a preexisting condition you don't have that causes you to be denied for medical or life insurance coverage
- You receive notice from the IRS that you filed more than one tax return or that you have income from an unknown employer
- You are notified that your information was compromised in a data breach

10 Steps Toward Recovery
Once you know there is a problem, take the following steps to minimize the damage.

1. **File a police report and notify the FBI and Federal Trade Commission (FTC)**.
A police report notifies local police of criminal activity and allows you to protect yourself if your information is used to commit a crime. You also can file an online complaint with the FBI's Internet Crime Complaint Center at https://complaint.ic3.gov/, and a report with the FTC at identitytheft.gov so information can be shared with law enforcement agencies.

2. **Notify the IRS and your identity theft insurance, if applicable**.
A *Form 14039 Identity Theft Affidavit* notifies the IRS if your Social Security number was used to file a fraudulent income tax return. If you've purchased an identity theft insurance policy, file a claim to help limit your financial losses. You may also have benefits through your homeowner or other insurance plan.

3. **Place a free fraud alert or security freeze on your credit reports**.
Request a free fraud alert from the three major credit bureaus—Experian, Equifax and TransUnion—to automatically notify any institution that pulls your credit report that your identity was compromised for one year. You will receive access to a free credit report from each bureau.

You can also request an extended fraud alert that lasts for seven years and allows you to receive two free credit reports from each bureau within 12 months.

- Equifax Alert online or call 1-800-525-6285
- Experian Fraud Center online or call 1-888-397-3742
- TransUnion Fraud Alert online or call 1-888-909-8872

A security freeze differs from a fraud alert because, instead of just notifying you of requests, it *prohibits* your credit report information from being released without your express approval. This prevents a credit bureau from approving new credit, loans or other services in your name without your authorization. If you have children, consider freezing their reports as well since they too can be victims of identity theft.

4. **Review credit card and bank statements for other unauthorized charges**.
Pull up statements for all of your accounts—including dormant or infrequently used accounts—and scan them for charges you don't recognize. Don't discount small amounts (e.g., $1). Sometimes thieves start small to see if the activity will be flagged before making large purchases. If you find unknown charges, notify your financial institution.

5. **Open new credit card and financial accounts.**
Close all of your accounts and open new ones (with new account numbers), even if all accounts haven't been compromised. This helps prevent a thief from gaining future control of your money.

6. **Tighten security on your accounts.**
Create new passwords for all of your accounts. Make sure each password is complex and unique. If you have a hard time remembering passwords, consider using a reputable password manager to ensure all your accounts have strong passwords. These services

generate passwords that cannot be easily guessed and then store and autofill them on websites so users don't need to remember each one.

7. **Take advantage of all of your rights under the Fair Credit Reporting Act (FCRA).**
The FCRA is a federal law designed to ensure fairness, accuracy and privacy of the personal information collected by credit bureaus. It regulates the collection of, and access to, consumer credit information. These rights include:

- Placing credit bureau fraud alerts and getting copies of your credit reports
- Placing a security freeze on your credit report
- Obtaining documents related to fraudulent transactions or accounts
- Obtaining information from debt collectors
- Blocking the damaging information so it doesn't appear in your credit reports
- Stopping businesses from reporting inaccurate information to the credit bureaus

8. **Alert your health insurance and medical care providers.**
Contact your providers to make sure your insurance information hasn't been fraudulently used to receive healthcare services—such as seeing a doctor, receiving prescription drugs, having surgery or visiting an emergency room.

9. **Contact your state's DMV or licensing agency.**
Ask your state's licensing agency to place a flag on your driver's license and/or ID number to notify law enforcement in case your ID is used fraudulently to write a check, during a traffic stop or to make a fake license.

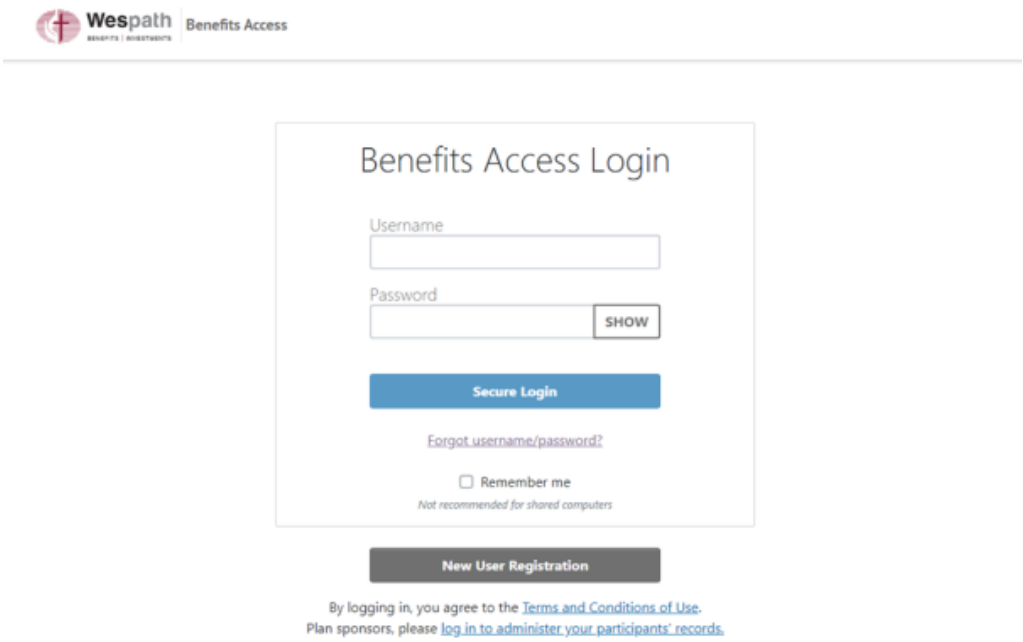
10. **Sign up for a credit monitoring service, if offered.**
If your information was accessed in a data breach, you may be offered complimentary credit monitoring, which alerts you to suspicious activity or new account openings. You can also pay for a reputable service, and some plans can limit or cover financial losses associated with identity theft.

If you need help developing a comprehensive identity theft recovery plan, visit the FTC's identity theft website.

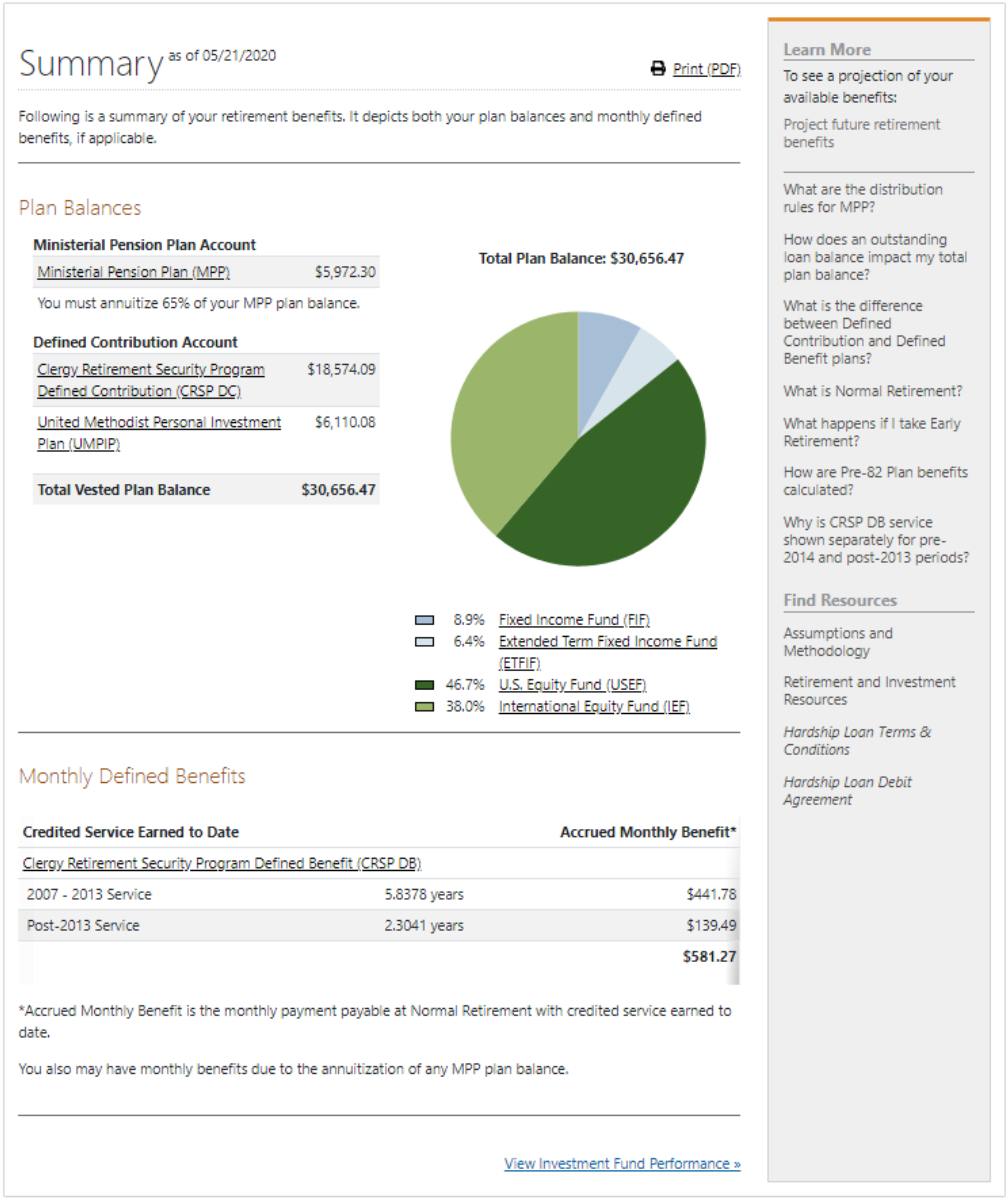
Sneak Peak: Benefits Access Updates

When you log into Benefits Access in early June, it will have a different look! We've redesigned the site to help you find information easily and more quickly. Below are the login and home pages. We will share additional information about the site updates, and more design sneak peaks next week. Stay tuned!

Login Page: The new login page features a streamlined and simplified design. While the look has changed, accessing the site remains the same—you will still use your current username and password.



Homepage: The new homepage provides instant access to your retirement account summary. Instead of having to search through menu options, you see your plan balances, investment allocation and monthly defined benefits, if any, at a glance.



Summary as of 05/21/2020

Print (PDF)

Following is a summary of your retirement benefits. It depicts both your plan balances and monthly defined benefits, if applicable.

Plan Balances

Ministerial Pension Plan Account

Ministerial Pension Plan (MPP)	$5,972.30

You must annuitize 65% of your MPP plan balance.

Defined Contribution Account

Clergy Retirement Security Program Defined Contribution (CRSP DC)	$18,574.09
United Methodist Personal Investment Plan (UMPIP)	$6,110.08
Total Vested Plan Balance	**$30,656.47**

Total Plan Balance: $30,656.47

Monthly Defined Benefits

Credited Service Earned to Date		Accrued Monthly Benefit*
Clergy Retirement Security Program Defined Benefit (CRSP DB)		
2007 - 2013 Service	5.8378 years	$441.78
Post-2013 Service	2.3041 years	$139.49
		$581.27

*Accrued Monthly Benefit is the monthly payment payable at Normal Retirement with credited service earned to date.

You also may have monthly benefits due to the annuitization of any MPP plan balance.

View Investment Fund Performance »

Learn More

To see a projection of your available benefits:

Project future retirement benefits

What are the distribution rules for MPP?

How does an outstanding loan balance impact my total plan balance?

What is the difference between Defined Contribution and Defined Benefit plans?

What is Normal Retirement?

What happens if I take Early Retirement?

How are Pre-82 Plan benefits calculated?

Why is CRSP DB service shown separately for pre-2014 and post-2013 periods?

Find Resources

Assumptions and Methodology

Retirement and Investment Resources

Hardship Loan Terms & Conditions

Hardship Loan Debit Agreement

For Your Education

Annuitization—What You Need to Know
Martin Bauer, Senior Managing Director of Benefit Plans, explains why retirees should feel safe knowing Wespath annuities are well-managed to support their retirement benefits now and in the future.

wespath.org

Our address is 1901 Chestnut Ave., Glenview, IL 60025, USA

To contact Wespath Benefits and Investments, click here.