Member Alert: High level of Fraud and Scams due to the COVID 19 crisis.

Investment scams:

A critical component of fighting investment fraud is investor awareness. To help investors identify common telltale signs of possible investment fraud, The Department of Financial Institutions suggest three questions to ask before making a new investment:

1. Is the investment being offered with a guaranteed high return with little or no risk? All investments carry risk that you may potentially lose some or all of your money. Anyone who says their investment offer has no risk is lying. No one can guarantee an investment return.

2. Is there a sense of urgency or limited availability of detailed information surrounding the investment? If someone offers you a “can’t miss” investment opportunity and pressures you to invest right now, don’t be afraid to walk away.

3. Is the person offering the investment, and the investment itself, properly licensed or registered? For the same reasons you wouldn’t go to an unlicensed doctor or dentist, you should avoid unregistered investment salespeople and their products.

Identity theft:

We want to provide information related to the massive identity theft operation occurring with the unemployment benefits claims process. It is clear that there is an identity theft ring operating to try and defraud the unemployment benefits process. This group has citizens' social security number, birth date, name and address. They most likely obtained this information during one of the large security breaches that have occurred over the past few years. They are now using this information to try to fraudulently obtain unemployment benefits.

Step One: Find out if you are affected.

If you received a letter from your state's unemployment office discussing your claim or if your company has notified you of a false claim, go to Step Two. Otherwise, go to your state's unemployment website and create an account or talk to someone to find out if a claim has been filed under your social security number.

Step Two: File a fraud claim with your state's unemployment department.

- Idaho: **https://www.labor.idaho.gov/dnn/Businesses/Report-Fraud**
- Oregon: **https://www.oregon.gov/employ/Unemployment/Pages/Fraud.aspx**
- Washington: **https://esd.wa.gov/unemployment/unemployment-benefits-fraud**

Step Three: Police Report

- File an online or non-emergency report with the agency whose jurisdiction you live in. (Spokane County - Crime Check 509-456-2233; other regions please file with your local crime reporting hotline.)
- Start keeping a file folder or journal with the information from this incident, including any case numbers. Some government services and accommodations are available to victims of identity theft that are not available to the general public, such as getting certain public records sealed.

Step Four: The Three Major Credit Bureaus

- Obtain your free credit reports from Equifax, Experian, and TransUnion at: **https://www.annualcreditreport.com/index.action** or call 1-877-322-8228.
- Report to the credit bureaus that the fraudulent claim was made using your identity and provide them with the case number from your police report. You can have a fraud alert put on your identity or freeze your credit. Doing either is free by law.
- A fraud alert is free and will make it harder for someone to open new accounts in your name. To place a fraud alert, contact one of the three credit bureaus. That company must tell the other two.
  - Experian 1-888-397-3742
  - TransUnion 1-800-680-7289
  - Equifax 1-888-766-0008
- Check your credit activity at least once a year. As a victim of identity-theft you have the right to check it monthly if you choose.
- Credit Freeze – If you do not have upcoming large purchases, such as a home, you may want to freeze your credit for more protection. It is free and you can do it yourself. To learn more about how to freeze your credit go to: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

Step Five: FTC & IRS

- File a short report with the FTC and give them the case number for your local police report. Go to: https://www.identitytheft.gov/
- Consider setting up an IRS account. If you create an account with your social security number it will prevent criminals from creating an account using your identity. Go to: https://www.irs.gov/payments/view-your-tax-account Near the middle of the page is a blue button that says "Create or view your account".
- Another option is to lock your social security number. The next wave of this cyber-attack may be IRS tax fraud.

Step Six: Keep Your Notes

- Hang on to any notes, copies of emails, etc. This is the paper trail that you can reference if you face any identity issues or locate inaccuracies on your credit history sometime in the future.

Step Seven: Consider signing up for Identity Theft/Credit Monitoring Services

- You can sign up with one of the public firms that offer credit monitoring services. Each credit bureau also offers credit monitoring services.

It is always sad to see people using a crisis to take advantage of cracks in the system. Identify theft is a real risk and that is what has happened if you have been swept into this fraud activity. As someone who has been affected by this fraudulent activity, I can tell you that it is a royal pain and time consuming to follow the above steps. It is, however, necessary in order to protect your credit and your financial health. I would also suggest that you change your password for your email accounts and any account that contains your financial information.

Thank you for reading these updates. Avista Credit Union's goal is to provide you with understandable and objective information to help as we all progress through this crisis and ultimate recovery. Please visit our website www.avistacu.com to stay current on information regarding the COVID-19 pandemic and what Avista Credit Union is doing to help you through this crisis.