Your Money. Your Identity. Your Protection.

At Fidelis - we're always looking out for you, our members—your financial well-being, as well as your financial and personal safety. So, this page is meant as a resource for you to visit from time-to-time to learn about security situations surrounding your financial information, as well as how Fidelis plays a role in your protection.

To start off, we want to share a few points with you from our end of protecting your safety, and suggestions to help you do so as well.

- We will never sell or share your information with any unnecessary third-party companies or vendors
- We will never ask you for highly sensitive information such as your Social Security Number, account numbers, etc. via email or any other non-secure virtual means
    - If you receive communication via these channels asking you for this type of information, it's most likely spam and we ask you to contact us directly as soon as possible
- When you are reaching out to us via email or any other non-secure virtual means, please do not share highly sensitive information such as your Social Security Number, account numbers, etc.
    - You may share with us your phone number, address, etc. if you are certain you are communicating with us directly, but we suggest not listing or sharing any personal information if you are looking to communicate with us via non-secure virtual means. We will directly contact you should we need this kind of information from you.
    - To report any suspected fraud or to notify us before traveling to avoid blocked transactions, please click here to contact us. www.fideliscu.org
- **Cyber Security Tips**
    - Avoid unknown links and attachments - Be very careful of websites, ads, and emails promoting free or discounted prices, and make sure to not click on any links or attachments you don't trust;
    - Check for https - When making online purchases, be sure the website is using the "https" protocol to confirm your information is secure;
    - Update Software - Keep all of your anti-virus software, browsers, and plug-ins up to date;

- Watch out for Wi-Fi - Be wary of the wireless networks you connect to while traveling. Connecting to a compromised network can lead to theft of your credentials and other personal information;
- Password Protect Devices - Be sure to secure mobile devices with a PIN or password. Devices left un-attended and without a password are easy targets for criminals.

- **At ATMS**
  - Be aware of your surroundings
  - If it looks like someone has tampered with the equipment, don't use it
  - If a suspicious person offers to help you use the ATM, refuse and leave
  - Put your money and ATM card away before you leave the ATM
  - Always avoid showing your cash and always verify that the amount you withdrew or deposited matches the amount printed on your receipt
  - Shred or destroy your ATM receipts before you throw them away
- **For Debit, ATM and Credit Cards**
  - Report lost or stolen cards immediately
  - Sign your card on the signature panel as soon as you receive it
  - Don't leave your credit cards in your car's glove compartment as a high percentage of credit card thefts are from car glove compartments
  - Keep your cards away from things with magnets, which can erase the information stored on the card's magnetic strip
- **PIN Safety**
  - Never write down your personal identification number (PIN), especially on the back of your card — instead memorize it
  - Don't write down your account number and PIN and carry it with you because if your wallet or purse is stolen, someone else could have access to your money
  - Never tell anyone your PIN
  - No one from Fidelis, the police or a merchant should ask for your PIN
  - When selecting a PIN, avoid picking a number that is easy for others to guess — for example, your name, telephone number, date of birth, or any simple combination of these
  - When typing in your PIN at the ATM or when making a point-of-sale purchase, cover the number pad so no one near you can see your PIN

- **ID Theft & Fraud**
  - Fidelis is here to help our members protect their personal information by providing information on the most recent ID Theft and Fraud issues and security breaches locally and nationally, as well as tips to keeping you safe online and out there in the world. But, at any time if

you need to report any suspected fraud or to notify us before traveling to avoid blocked transactions, please click here to contact us. www.fideliscu.org

NCUA Fraud Prevention Center

The National Credit Union Administration (NCUA) now provides a wonderful resource for credit union members covering a variety of frauds and scams, identity theft and online security information and protection measures. Click here to view information this very helpful personal and financial protection tool. www.mycreditunion.gov

Contact Fidelis directly if you are concerned that your account information or Credit or Debit Card may be compromised.

Fidelis Catholic Credit Union
6320 Olde Wadsworth Blvd.
Arvada, CO. 80003
Phone: 303-424-5037
Fax: 303-422-0116
Email: Memberservices@fideliscu.org
Or contact us securely through messaging on your Fidelis Online Banking Account.

To Report Credit or Debit Card Fraud or if your card is Lost or Stolen after Credit Union Hours: Please call 1-800-543-5073.

Excerpts from IRS Website 2IR-2018-27, Feb. 13, 2018

Scam Alert: IRS Urges Taxpayers to Watch Out for Erroneous Refunds; Beware of Fake Calls to Return Money to a Collection Agency

WASHINGTON — The Internal Revenue Service today warned taxpayers of a quickly growing scam involving erroneous tax refunds being deposited into their bank accounts. The IRS also offered a step-by-step explanation for how to return the funds and avoid being scammed.

Following up on a Security Summit alert issued Feb. 2, the IRS issued this additional warning about the new scheme after discovering more tax practitioners' computer files have been breached. In addition, the number of potential taxpayer victims jumped from a few hundred to several thousand in just days. The IRS Criminal Investigation division continues its investigation into the scope and breadth of this scheme.

These criminals have a new twist on an old scam. After stealing client data from tax professionals and filing fraudulent tax returns, these criminals use the taxpayers' real bank accounts for the deposit.

Thieves are then using various tactics to reclaim the refund from the taxpayers, and their versions of the scam may continue to evolve.

Different Versions of the Scam

In one version of the scam, criminals posing as debt collection agency officials acting on behalf of the IRS contacted the taxpayers to say a refund was deposited in error, and they asked the taxpayers to forward the money to their collection agency.

In another version, the taxpayer who received the erroneous refund gets an automated call with a recorded voice saying he is from the IRS and threatens the taxpayer with criminal fraud charges, an arrest warrant and a "blacklisting" of their Social Security Number. The recorded voice gives the taxpayer a case number and a telephone number to call to return the refund.

As it did last week, the IRS repeated its call for tax professionals to step up security of sensitive client tax and financial files.

The IRS urged taxpayers to follow established procedures for returning an erroneous refund to the agency. The IRS also encouraged taxpayers to discuss the issue with their financial institutions because there may be a need to close bank accounts. Taxpayers receiving erroneous refunds also should contact their tax preparers immediately.

Because this is a peak season for filing tax returns, taxpayers who file electronically may find that their tax return will reject because a return bearing their Social Security number is already on file. If that's the case, taxpayers should follow the steps outlined in the Taxpayer Guide to Identity Theft located on the IRS website. Taxpayers unable to file electronically should mail a paper tax return along with Form 14039, Identity Theft Affidavit, stating they were victims of a tax preparer data breach.

Here are the official ways to return an erroneous refund to the IRS.

Taxpayers who receive the refunds should follow the steps outlined by Tax Topic Number 161-Returning an Erroneous Refund at www.IRS.gov. Tax topic contains full details, including mailing addresses should there be a need to return paper checks. By law, interest may accrue on erroneous refunds.

If the erroneous refund was a **direct deposit**:

1. Contact the Automated Clearing House (ACH) department of the bank/financial institution where the direct deposit was received and have them return the refund to the IRS.
2. Call the IRS toll-free at 800-829-1040 (individual) or 800-829-4933 (business) to explain why the direct deposit is being returned.

If the erroneous refund was a **paper check** and hasn't been cashed:

1. Write "Void" in the endorsement section on the back of the check.
2. Submit the check immediately to the appropriate IRS location listed below. The location is based on the city (possibly abbreviated) on the bottom text line in front of the words TAX REFUND on your refund check.
3. Don't staple, bend, or paper clip the check.
4. Include a note stating, "Return of erroneous refund check because (and give a brief explanation of the reason for returning the refund check)."

The erroneous refund was a paper check and **you have cashed it**:

- Submit a personal check, money order, etc., immediately to the appropriate IRS location listed below.
- If you no longer have access to a copy of the check, call the IRS toll-free at 800-829-1040 (individual) or 800-829-4933 (business) (see telephone and local assistance for hours of operation) and explain to the IRS assistor that you need information to repay a cashed refund check.
- Write on the check/money order: Payment of Erroneous Refund, the tax period for which the refund was issued, and your taxpayer identification number (social security number, employer identification number, or individual taxpayer identification number).
- Include a brief explanation of the reason for returning the refund.
- Repaying an erroneous refund in this manner may result in interest due the IRS.

IRS mailing addresses for returning paper checks

For your paper refund check, here are the IRS mailing addresses to use based on the city (possibly abbreviated). These cities are located on the check's bottom text line in front of the words TAX REFUND:

- ANDOVER – Internal Revenue Service, 310 Lowell Street, Andover MA 01810
- ATLANTA – Internal Revenue Service, 4800 Buford Highway, Chamblee GA 30341
- AUSTIN – Internal Revenue Service, 3651 South Interregional Highway 35, Austin TX 78741
- BRKHAVN – Internal Revenue Service, 5000 Corporate Ct., Holtsville NY 11742
- CNCNATI – Internal Revenue Service, 201 West Rivercenter Blvd., Covington KY 41011
- FRESNO – Internal Revenue Service, 5045 East Butler Avenue, Fresno CA 93727
- KANS CY – Internal Revenue Service, 333 W. Pershing Road, Kansas City MO 64108-4302
- MEMPHIS – Internal Revenue Service, 5333 Getwell Road, Memphis TN 38118

- OGDEN – Internal Revenue Service, 1973 Rulon White Blvd., Ogden UT 84201
- PHILA – Internal Revenue Service, 2970 Market St., Philadelphia PA 19104