

DFCU will never ask you to give your personal and confidential information through an email, text, or voice message. If we initiate contact with you, then we already have this information on record and would have no need to ask you for it.

How to Protect yourself from ID theft

Identity theft has become an alarming problem which no one should ignore. Identity thieves may try to pose as a financial institution or credit card company employee over the phone but doing so should be a dead giveaway. Legitimate organizations will not call and ask you for personal information—like your ATM or Debit Card PIN number, your Social Security number, or your online banking credential.

Even if you suspect a call might be legitimate, ask for the caller's credentials, hang up, and contact the organization using the phone number listed on your financial institution's bank statements or the one on the back of your Credit/Debit Card. If the caller gives you a different phone number to call back that you do not recognize, be suspicious.

Callers can get aggressive – telling you that you will go to jail or that you owe lots of money. They are trying to scare you into giving them your personal information. Do not let them intimidate you. Hang up and call your financial institution.

To learn more about identity theft fraud safety visit www.idtheftcenter.org

If you think you have been a victim of identity theft, contact the Federal Trade Commission (FTC) at 877-IDTHEFT (438-4338) or visit www.ftc.gov/idtheft. If you believe your Social Security Number is being used fraudulently contact the Social Security Administration at 800-772-1213. Contact your local law enforcement to file a police report. Record the police department name and case number.

It is a good idea to get a copy of your credit report each year from each credit-reporting agency. The three major agencies are:

- **Experian:** www.experian.com; credit report copy - 888-397-3742; fraud unit - 888-397-3742
- **Equifax:** www.equifax.com; credit report copy - 800-685-1111; fraud unit - 800-525-6285
- **TransUnion:** www.transunion.com; credit report copy - 800-888-4213; fraud unit - 800-680-7289
- Visit the website www.annualcreditreport.com for a free credit report (Please note: one free credit report per year).

Check your credit report regularly.

Credit reports include the activity on any accounts in your name, including the last-reported balances and any newly opened accounts. Check your credit report regularly, and if you notice something suspicious, like an unfamiliar account, take action to address it as soon as possible.

Choose Complex Personal Passwords.

Do not use something that is easily guessed, like your date of birth, mother's maiden name, or the last four of your social security number as a password. Try to include special characters and numbers in your passwords. And be sure to change your passwords on a regular basis. Enable and use dual factor authenticator feature when possible, to increase security.

Make a Copy of Your IDs.

Make a copy of your driver's license, Social Security card, birth certificate, passport etc. and store them in a safe place where you can get to them when you need them.

Store Original Documents and IDs in a Safe Place.

Do not carry your Social Security number card with you in your wallet; leave it in a secure place. Same goes for IDs and documents that you do not need regularly, like passports and birth certificates.

Opt-Out of Pre-screening of your Credit Reports.

The number to call is 1.888.567.8688 (1.888.5OPTOUT). It requires one single call for all three credit bureaus. This will stop the arrival of pre-approved credit card offers in your mailbox.

Be Aware of Phishing and Spoofing Attempts.

Scammers can make calls or send texts that appear to come from government entities, businesses, or familiar phone numbers, and emails that appear to be legitimate, in an attempt to steal your information. Contact the company using a phone number or website that you know is legitimate.

Treat Your Mail Carefully.

Avoid leaving mail in your mailbox, as that is a frequent target of identity thieves. You might also consider limiting how much paper mail you receive in the first place by signing up for electronic statements. And when mailing outgoing bill payments or checks, it is safest to mail them from the post office or another secure location, as opposed to placing them in your mailbox for pick up.

Shred Your Personal Information.

To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear, or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you are discarding, and credit offers you get in the mail.