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.

Card Fraud

If you are a DFCU card holder (Debit/Credit) and you suspect fraudulent activity on your account, you should contact us immediately:

Contact any Branch during regular business hours.

Or call us Monday – Saturday: 24-hour a day Sunday: 24-hour card support only Salt Lake Area: <u>801-456-7000</u> Toll-Free: <u>800-326-3328</u>

Skimming

Skimming is a method by which thieves steal your credit card information. These devices read the information obtained on the magnetic strip of your credit/debit card. This information is then sold, and counterfeit cards are made. Thieves then use these "cloned" credit cards to make purchases. Often times, victims are unaware of these purchases until a statement arrives in the mail (or you're denied purchases) and the cardholder notices the fraudulent charges/withdrawals. Skimming devices placed on ATM skimming machines often involve the "skimmer" itself and a camera strategically placed to record the four-digit PIN number that the cardholder uses. This way, once cloned debit cards are produced, thieves have the corresponding 4-digit PIN to withdraw cash. Hence, you never lose possession of your card!

What to look for (ATM skimming):

- 1. Inspect the door access device prior to opening the lobby doors (Most counterfeit devices are installed with double sided tape and are installed over the original door access device)
- 2. Inspect the machine for items that were installed over or around the PIN pad of the ATM. Customers should be looking for an attachment on the ATM that contains a small hole (camera) that is pointed in the direction of the PIN pad. If possible, use your other hand to block the numbers you are entering on the PIN pad.
- 3. Card slot of the ATM is loose or has fallen off, or other parts of the ATM machine have dislodged from the ATM.
- 4. Pay attention to person(s) attaching, removing, or tampering with parts of the ATM machine.

You should also note:

- 1. Most skimmers are installed on Saturdays and Sundays when most Financial Institutions are closed.
- 2. Thieves who install these devices are very often lurking somewhere nearby to keep an eye on their investment.

What to do if you are the victim:

- Call the local police and file a report
- Contact your credit union/bank or credit card issuer immediately and tell them your card data has been stolen.
- Contact the three major credit bureaus to request a security freeze, which prevents new credit authorizations without your consent.
 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 <u>www.annualcreditreport.com</u> for a free credit report (Please note: one free credit report per year).

DO NOT remove a skimming device if detected, contact local police.