



Dominion Energy
Credit Union®

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

15957

October 29, 2019



F0138-L01-0000001 P001 T00002 *****MIXED AADC 159

SAMPLE A SAMPLE - L01

APT 123

123 ANY ST

ANYTOWN, US 12345-6789



RE: Important Security Notification
Please read this entire letter.

Dear Sample A Sample:

We are contacting you regarding a data security incident that occurred on May 14, 2019 at Geezeo, a Dominion Energy Credit Union ("DECU") service provider, which may have exposed your personal information to others. This incident may have involved your name, email address, account balance, birth year, or account number. No passwords, PINs, or access codes were involved, and, as described below, the compromised file did not specifically identify your account number as a DECU account. However, it is possible that reference data included in the compromised file could be used to identify your account number as being associated with DECU. Please be assured that we have taken every step necessary to address the incident.

What happened:

We were notified on September 30, 2019 by Geezeo of unusual activity involving a third-party service provider of Geezeo's. As a service provider for DECU, Geezeo provides the Money Manager services of our online banking website. Geezeo's vendor notified Geezeo of the unusual activity in early September, and Geezeo immediately launched an investigation to assess what occurred. Geezeo was able to determine that on May 14, 2019, an unauthorized party accessed user data from a 2012 backup data file stored at Geezeo's vendor. The file contained the information of approximately 97 financial institutions, and DECU is one of these affected financial institutions. Geezeo took immediate steps to block further access by unauthorized parties and implemented enhanced security across their platform.

As noted above, it does *not* appear that the backup file contained any password, security code, access code or other similar information that would permit access to a consumer's financial account. While the account numbers in the compromised files were not specifically identified as DECU account numbers, the files also contained Geezeo reference data that could be used to identify the account numbers as being associated with DECU.

What we are doing to protect your information:

When we learned what happened, we immediately set up multifactor authentication for access to member data environments, employed network and firewall segregation between member data containing networks with access to the internet, flagged affected accounts, and ensured Geezeo closed the method through which the bad actor was able to access your data. Under our written information security program, we also use Intrusion



F0138-L01

Detection Systems, scan for vulnerabilities, and monitor database access. We will continue to annually review critical vendors like Geezeo to ensure that they are following the best cybersecurity practices. In addition, Geezeo has taken steps to block further access by unauthorized parties, has implemented enhanced security across its platform, and has notified law enforcement.

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: January 31, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-281-4826 by **January 31, 2020**. Be prepared to provide engagement number **DB15173** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-281-4826. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

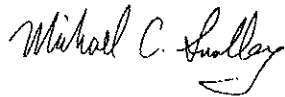
Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

We encourage you to take advantage of the identity monitoring services we are offering you. Also, we have enclosed Tips to Safeguard Personal Information which provides general information on how to protect your identity and your sensitive consumer information.

It is important that you remain vigilant over the next 12 to 24 months to identify and address any possible misuse of your personal information. In the unfortunate event your personal information is misused or you suspect you are a victim of identity theft, please promptly report the incident to Dominion Energy Credit Union and please call the toll free number above to receive the identity repair services from Experian that are available to you, free of charge for one year.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at (800) 268-6928. We have posted FAQs about this incident on our website at www.dominionenergycu.org/MoneyManagerIncident.

Sincerely,



Michael C. Swalley
CEO of Dominion Energy Credit Union

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

0000001



F0138-L01

Tips to Safeguard Personal Information

Protecting your accounts	<ul style="list-style-type: none">• Monitor your account statements often (even daily in online banking) to review all charges and transactions. Contact Dominion Energy Credit Union immediately if you see any discrepancies or unauthorized or suspicious activity.• If available, place password protection on all your accounts, and do not use any part of your social security number as the username or password.• Do not write down or share your Personal Identification Number (PIN) number or passwords with anyone.• For more tips on how to protect your accounts, please visit https://www.consumer.ftc.gov/features/feature-0014-identity-theft• Be cautious of email messages requesting you to divulge information about your account or prompting you to provide personal information, as such emails could be phishing attacks. For more guidance, please refer to the Department of Homeland Security's guidance available at https://www.us-cert.gov/report-phishing or the Federal Trade Commission's guidance available at https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.			
Protecting your identity	<ul style="list-style-type: none">• You may place a fraud alert on your credit file by contacting the fraud departments of the three nationwide credit reporting agencies, which prompts any issuer of credit to use additional scrutiny for any request for new or increased credit. This provides a significant layer of protection; however, it may limit your ability to get "instant credit" such as the offers often available at retail stores.• Check your credit report to ensure all your information is correct. You can obtain a free credit report from each of the nationwide consumer credit reporting agencies every 12 months by visiting www.annualcreditreport.com or calling 1-877-322-8228. You may want to obtain copies of your credit report to ensure the accuracy of the report information. When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report.• If you believe you are a victim of identity theft, report it to your local law enforcement and to the FTC (see their contact information below) or your state Attorney General and one of the three nationwide consumer reporting agencies listed below to have it removed from your credit file.• For more information about steps to take, including requesting fraud alerts, security freezes, or credit reports, contact:<table><tr><td>Equifax Information Services LLC: 1-800-525-6285 or www.equifax.com P.O. Box 105069 Atlanta, GA 30348-5069</td><td>Experian: 1-888-397-3742 or www.experian.com P.O. Box 9532 Allen, TX 75013</td><td>TransUnion: 1-800-680-7289 or www.transunion.com P.O. Box 2000 Chester, PA 19016</td></tr></table>• Learn more about steps you can take to protect against identity theft from the Federal Trade Commission at www.consumer.ftc.gov/topics/identity-theft. Or call the FTC's Identity Theft Hotline toll-free at 1-877-IDTHEFT (1-877-439-4339)	Equifax Information Services LLC: 1-800-525-6285 or www.equifax.com P.O. Box 105069 Atlanta, GA 30348-5069	Experian: 1-888-397-3742 or www.experian.com P.O. Box 9532 Allen, TX 75013	TransUnion: 1-800-680-7289 or www.transunion.com P.O. Box 2000 Chester, PA 19016
Equifax Information Services LLC: 1-800-525-6285 or www.equifax.com P.O. Box 105069 Atlanta, GA 30348-5069	Experian: 1-888-397-3742 or www.experian.com P.O. Box 9532 Allen, TX 75013	TransUnion: 1-800-680-7289 or www.transunion.com P.O. Box 2000 Chester, PA 19016		