

Good afternoon:

I am emailing on behalf of Destinations Credit Union. Please read the attached documents regarding an email incident that occurred with a third-party vendor. We have notified NCUA as well as our Cyber Security Insurer. We are also attaching the member communication being mailed to 105 members.

If you should have any questions, please contact me.

Thank you.



Trish Fluke
Operations Manager

 [410-663-2500](tel:410-663-2500) Ext. 116 |  [410-663-2150](tel:410-663-2150) |  www.destinationscu.org



**The information transmitted may contain confidential material and is intended only for the person or entity to which it is addressed. Any review, retransmission, dissemination, or other use of, or taking of any action by persons or entities other than the intended recipient is prohibited. If you are not the intended recipient, please delete the information from your system and contact the sender.*

- **Reporter Name and Title:** Trish Fluke, Operations Manager
- **Callback Number:** Work number: (410) 663-2500 ext 116
- **Credit Union Name:** Destinations Credit Union
- **Date and Time Identified:** The incident occurred on April 1st, 2024. rkGoBig, our credit union CUSO, sent an email notification on April 8th at 8pm which was seen the morning of April 9th. Kamala Brody, Chief Compliance Officer for rkGoBig reported the incident to NCUA on behalf of the CUSO credit unions on April 9. We were notified of the members who were exposed the afternoon of April 9th. Destinations immediately started working this as a reportable event.
- **Description:** A general description of the reportable cyber incident:
 - **General description**
 - The event was a BEC by business partner rkGoBig. On Monday, April 1st, an employee of rkGoBig became the victim of a malicious email. The employee clicked on a link and provided credentials to the mailbox. The mailbox included data of various credit union members.
 - **What services were impacted?** NONE
 - **Was sensitive data or member information compromised?**
 - Cannot be determined at this time
 - **What impact did it have on operations?**
 - No impact on operations



Notice of Information Security Incident

DATE

MEMBER NAME

ADDRESS

ADDRESS

Dear MEMBER

We value your privacy and make every effort to keep your personal information safe. Unfortunately, we're writing today to let you know about a recent incident regarding your personal information.

What Happened? A third-party service provider recently notified us of an information security incident occurring on or around April 1, 2024, that may have placed sensitive member information at risk for misuse. The incident impacted a very limited number of Destinations' memberships; however, your account was identified as possibly vulnerable. We realize this is not the news you want to hear. Safeguarding personal information is something we take very seriously.

What Information Was Involved? Information on your account, including your name, address, phone number and account number were identified as items possibly at risk.

What Are We Doing? This incident is being addressed through an internal investigation by our third-party service provider. To date, there is no evidence that sensitive member information was improperly accessed; however, this notice is sent in order that you may take some precautions. If you call the credit union in the future, you can expect to be asked different security questions before gaining access to your account.

What Can You Do? We recommend the following measures to protect yourself from identity theft and fraud:

- Do not provide your personal information such as date of birth, account number, debit or credit card number or social security number in response to a phone call, email, or text. We will not contact you and request that information. We will verify your identity by using other methods if we call you or you call us.
- Be wary of emails or texts requiring you to open a link or document. Fraudsters use these methods to introduce malware to your device.
- If you are contacted by anyone regarding your account, we encourage you to obtain their name, disengage from contact and call us at 410-663-2500 to verify they are calling on behalf of the credit union.
- Remain vigilant for incidents of fraud, identity theft, and errors by regularly reviewing your account statements for any unauthorized activity.
- **Establish a new code word on your account(s). Also, routinely change online account passwords and security questions.**

- **If you wish, Destinations will reassign you with a new account number upon your authorization. This is the best option to protect the integrity of your account – but it could impact your credit score. Contact us at 410-663-2500 to learn more about this process.**
- Report any suspicious or unauthorized activity to law enforcement and to the Federal Trade Commission (FTC) at 1-877-FTC-HELP (1-877-382-4357).
- Carefully monitor your credit report. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months. You may also have information relating to fraudulent transactions deleted from your credit report.
- Place a free fraud alert or security freeze on your credit file, which tells creditors to contact you before they open any new accounts or change your existing accounts – and alerts them of possible fraudulent activity. Fraud alerts last 90 days unless you manually renew them or use an automatic fraud alert feature. You can contact the credit reporting agencies directly at:

EQUIFAX
800-525-6285
PO Box 470241
Atlanta GA 30374-0241
www.equifax.com

EXPERIAN
888-397-3742
P.O. Box 2104
Allen, TX 75013-0949
www.experian.com

TRANSUNION
800-888-4213
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Additional information about credit reports and ways to prevent identity theft and fraud is available through the FTC at <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>, by visiting www.annualcreditreport.com, by calling 1-877-322-8228, by mail to: Federal Trade Commission Consumer Response, 600 Pennsylvania Avenue, Washington, DC 20580 or by contacting the Maryland Office of the Attorney General's Identity Theft Unit: Phone: 410-576-6491, Email: idtheft@oag.state.md.us, Mail: 200 St. Paul Place, 25th Floor, Baltimore MD 21202.

Again, we apologize for any concern or inconvenience this may cause. Thank you for your patience and understanding.

Respectfully yours.



Brian J Vittek
President/CEO