1. **What happened?**

Popular has been informed by one of our third-party vendors that it was a victim of a cybersecurity breach that included Popular files maintained by that vendor. Specifically, Popular's vendor used software owned by Accellion Inc. for secure file transfers with its customers, including Popular. The third-party software used by our vendor was compromised, resulting in unauthorized access to data maintained by the vendor.

Upon learning of the incident, the vendor immediately launched an investigation with the help of external cybersecurity experts and ceased using the Accellion software. The vendor's investigation ultimately revealed that certain of the files compromised in the incident included some personal information of Popular customers.

Your security, including protecting your personal information, is a top priority for Popular. Popular requires all of its vendors to maintain appropriate security measures to help prevent unauthorized access to personal information. Unfortunately, many companies and organizations, including this vendor, were impacted by the compromise of the Accellion software.

2. **Did the incident impact Popular's network or systems?**

Popular's own network and systems were not impacted by this incident.

3. **What types of personal information were impacted?**

Popular is sending each affected individual a letter that identifies the impacted information of such individual.

4. **How do I know if I am one of the affected customers?**

If you are one of the affected customers, Popular will contact you directly by U.S. Mail. Not all Popular customers were affected by this incident.

5. **What should I do if I receive an email or other communication claiming to be from Popular?**

Popular is notifying individuals affected by this incident via U.S. Mail. As always, customers should remain alert for suspicious e-mails or communications asking them to provide information about themselves or their accounts. If you receive a suspicious e-mail or communication, you should ignore it, or contact Popular using the official contact information located on its website, https://www.popular.com/en/contact-us, or by visiting a Popular branch. For more information about how to protect yourself, please visit Popular's online security hub at https://www.popular.com/en/security.

6. What services are being offered in response to this event?

Popular is offering individuals whose personal information has been exposed as part of this incident the ability to complimentarily enroll in two-year credit and identity monitoring services through Experian. Enrollment instructions for these services are included in the notification that Popular is providing by U.S. Mail to affected individuals. If you receive a letter and choose to take advantage of these services, you must complete the enrollment process described in the letter. The deadline to enroll is November 30, 2021.

7. Will enrolling in credit monitoring impact my credit score?

No, it will not impact your credit score.

8. What else can I do in response to the exposure of my personal information?

You should remain vigilant for the next 12 to 24 months for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you identify any suspicious or unusual activity on your accounts or suspect identity theft or fraud, report it immediately to your financial institutions.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you identify information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by visiting www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.Equifax.com/personal/credit-report-services

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.Experian.com/help

TransUnion
(888) 909-8872
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19022
www.TransUnion.com/credit-help

In addition, you may obtain additional information from the Federal Trade Commission ("FTC") and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies at the phone numbers above to place a security freeze to restrict access to your credit report.

9. Can I contact someone for more information?

Yes – you may contact us at (888) 258-0452 to receive further information or credit monitoring enrollment assistance.