tapestry

May 30, 2024

10 Hudson Yards, New York, NY 10001

Dear Employee,

We are writing to notify you about an issue that affected certain of your Tapestry gift card information. We recently became aware that Tapestry was the target of a phishing campaign. Phishing messages seek to trick individuals into clicking on a link and/or providing information (such as login credentials) to an unauthorized source. Based on our investigation, we determined that, in late March 2024, an unauthorized party used stolen account credentials of some Tapestry employees acquired through phishing tactics to gain access to certain Tapestry gift card information. The unauthorized party may have accessed your name and details associated with your Tapestry gift card (i.e., gift card number, PIN and expiration date). Importantly, we have no evidence that the unauthorized party used your Tapestry gift card to engage in fraudulent transactions.

Promptly after learning of the issue, we took steps to block unauthorized access to the affected Tapestry employee accounts. We also launched an investigation with the assistance of a third-party cybersecurity expert to understand the full nature and scope of the issue. We are taking steps to enhance our access controls and other security measures to help prevent further unauthorized access. In addition, we have replaced your relevant Tapestry gift card to help prevent misuse.

We take our obligation to safeguard personal information very seriously and are alerting you about this issue so you can take steps to help protect your information. We recommend that you:

- Refrain from using the same password you use for your Tapestry account on any other account (such as personal email accounts).
- Be cautious of any unsolicited communications (such as emails or text messages) that ask for your personal information or refer you to a web page asking for personal information.
- Avoid clicking on links or downloading attachments from suspicious emails and text messages.

If you need to obtain a new gift card, please contact Customer Care at 1-866-999-5283.

The attached Reference Guide also provides additional information and resources on the protection of personal information.

We regret any inconvenience this issue may cause you. If you have any questions regarding this matter, please contact Gedas Ramanauskas at 646-899-9540.

Sincerely,

Privacy Office

tapestry

U.S. Reference Guide

Placing a Fraud Alert on Your Credit File. You may wish to place a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies.

Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

For more information on fraud alerts, you also may contact the U.S. Federal Trade Commission ("FTC"):

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth

- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

Additional Information. Individuals may further educate themselves regarding identity theft and the steps they can take to protect their personal information by contacting the consumer reporting agencies or the FTC as described above, or their state Attorney General. Instances of known or suspected identity theft or fraud should be reported to law enforcement, the FTC and your state Attorney General. Individuals also have the right to file a local police report if they experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft or fraud, individuals may need to provide some proof that they have been a victim. This notice has not been delayed by law enforcement.

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
https://ag.ny.gov

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
https://ag.ny.gov/resources/individuals/consumer-issues/technology

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
(202)-727-3400
www.oag.dc.gov