



Charles Blanchard
Assistant Vice President – Senior Legal Counsel
charles.blanchard@att.com

AT&T Services, Inc.
One AT&T Plaza
208 S. Akard
Floor 30, Room 3063
Dallas, Texas 75202
214-757-3348

February 24, 2023

Email: Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Notice of Data Incident

Please take this letter as notice of a data security incident involving one (1) Maryland resident. On February 10, 2023, following vendor's investigation and report to AT&T, it was determined that an AT&T vendor employee inappropriately retained and reused Personal Identifying Information (PII) of an AT&T customer. Specifically, in violation of Company's policies and practices, this vendor employee appears to have improperly retained payment card information of a Maryland customer on or about 8/30/2022 and then used that information for two personal purchases.

Upon notice, the vendor took action to address the issue and restore integrity, including employment action, audit, training, and removal of certain software to enhance security. Additionally, AT&T is offering one year of credit monitoring and identity theft insurance to the affected customer at no cost.

A copy of the notice letter to be sent to the customer is attached.

We sincerely apologize for any inconvenience experienced by our customer and are committed to continued protection of our customer's security and privacy.

If you have any questions, please feel free to contact me.

Thanks very much.

Sincerely,

/s/ Charles Blanchard

Charles Blanchard
Assistant Vice President – Senior Legal Counsel



[DATE]

[NAME]

[ADDRESS]

[CITY], [STATE] [ZIP]-[ZIP+4]

RE: Notice of Data Breach

Dear [NAME]:

AT&T's commitment to customer privacy and data security is a top priority. As a follow-up to your initial complaint, we recently identified that one of our vendor employees violated our strict privacy and security guidelines. On behalf of AT&T, please accept my apology for this incident. Simply stated, this is not the way we conduct business.

What Happened

On or after 8/30/2022, a vendor employee inappropriately retained and reused your Personal Identifying Information (PII) without authorization.

What Information Was Involved

Your payment card was used without your authorization for the vendor's personal purchases.

What We Are Doing

The vendor has taken appropriate action with the individual who used your information in violation of our policies and guidelines.

To help address any inconvenience this may cause, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. **While we have already arranged for payment, you must enroll to start the service.** The attached page provides details about the service, as well as instructions on how to enroll online using your activation code and engagement number. If you have questions or concerns, please contact Experian at 855.223.4826 where specialists are ready to assist you.

What You Can Do

You may also want to consider contacting the major credit reporting agencies to place a fraud alert on your credit report, and to learn about identity theft programs offered by the Federal Trade Commission. Details on how to contact the credit reporting agencies and FTC can also be found on the attached pages.

If you would like to change your passcode and/or increase the security level of your account, you can do this online at www.att.com or via the app MyAT&T.

For More Information

We have a special dedicated team who will be happy to answer any questions you may have. You may reach them at 877.686.1457 weekdays between 8 a.m. and 6 p.m. Eastern time.

Thank you,

Rachel J. Ennis
Sales Director – Customer Advocacy & Service

IdentityWorksSM

After you complete registration for Experian's service, that AT&T is providing for you at no charge, you will have increased visibility into any possible fraudulent activity so you can respond more quickly if such activity is detected. You will also have an insurance policy of up to \$1,000,000 in coverage should you experience identity theft, and an Identity Restoration team to guide you through the recovery process.

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** **[MM/DD/YYYY]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: ExperianIDWorks.com/3bplus
- Provide your **activation code:** **[ACTIVATION]**

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 855.223.4826 by **[MM/DD/YYYY]**. Be prepared to provide engagement number **[ENGAGE]** as proof of eligibility for the identity restoration services by Experian.

IdentityWorksSM includes:

- **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.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **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.

Please note that 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 ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Fraud Alerts

In addition to completing IdentityWorksSM registration, AT&T strongly suggests that you contact the fraud departments of any one of the three major credit reporting agencies and let them know you may have potentially experienced identity theft. That agency will notify the other two. Through that process, a "fraud alert" will automatically be placed in each of your three credit reports to notify creditors not to issue new credit in your name without gaining your permission. Contact:

<u>Equifax</u>	<u>Experian</u>	<u>TransUnionTM</u>
P.O. Box 740241 Atlanta GA 30374 877.478.7625 www.fraudalerts.equifax.com	P.O. Box 2002 Allen, TX 75013 888.397.3742 www.experian.com	P.O. Box 6790 Fullerton, CA 92834 800.680.7289 www.transunion.com

We also encourage you to carefully review your credit report(s). Look for accounts you did not open and inquiries from creditors that you did not initiate. Also review your personal information for accuracy, such as home address and Social Security number. If you see anything you do not understand or that is inaccurate, call the credit reporting agency at the telephone number on the report. If you find suspicious activity on your credit reports or bank account, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need copies of the police report to clear your personal records. You can also request information from the agencies about the option of placing a security freeze on your credit reports.

Learn about the FTC's identity theft programs at www.ftc.gov/bcp/edu/microsites/idtheft or call the FTC's toll-free Identity Theft helpline: 877.ID.THEFT (877.438.4338); TTY: 866.653.4261.