Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.479.6700
f +1 215.665.8475

kennedyslaw.com

t +1 267 479 6706

Joshua.Mooney@kennedyslaw.com

February 28, 2025

By Webform Attachment

Attorney General Bob Ferguson
Office of the Attorney General'
For the State of Washington
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504
SecurityBreach@atg.wa.gov

Re: Notice of Data Breach

Dear Attorney General Ferguson:

Our office writes on behalf of our client, Transak USA LLC, to provide notice for a data breach impacting the personally identifiable information of 592 Washington residents.

On September 23, 2024, Transak, Inc. (Transak USA's parent) received a claim from an unknown individual alleging an unauthorized access and acquisition of Transak data hosted by a third party. Transak, Inc. initiated an investigation to substantiate the claim, including contacting the data host and requesting evidence of proof from the actor. It also retained a leading IT forensic firm – CrowdStrike - and our firm to assist with the investigation. Transak, Inc. learned that the credentials of a single employee were compromised allowing access to the third-party platform hosting the data. That employee's credentials no longer have access to any Transak system or the platform. Through the investigation, it has been confirmed that the compromise took place between September 1-11, 2024, and that there was an acquisition of data of 23,113 Transak USA LLC customers, including 592 Washington residents. The data included names, driver license numbers, and date of birth.

On October 20, 2024, Transak, Inc. learned that the actor published some of the data. Transak USA LLC is notifying the individuals whose PII was impacted and is offering complimentary credit monitoring services. Transak, Inc. also has contacted global law enforcement agencies, including the Department of Homeland Security and the FBI.

Since the event, Transak, Inc. has implemented additional or strengthened pre-existing security measures on Transak systems, including enforcing hardware-based MFA for accessing third-party vendor platforms where sensitive data is stored; implementing VPN security

enhancements; improving EDR monitoring, including with its KYC vendor; and implementing endpoint security upgrades and updated its access privilege modules. Transak, Inc. is also requiring more frequent security audits of its third-party vendors to ensure compliance with its enhanced security standards, and is implementing employee training to mitigate the risk of another cybersecurity event.

Should you have any further questions, please do not hesitate to contact me. Thank you.

Very truly yours,

/s/Joshua A. Mooney

Joshua A. Mooney

Partner
for Kennedys

cc: Annslee Perego, Esquire (Annslee.Perego@kennedyslaw.com)

Transak USA LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

February 26, 2025

Re: ***Notice of Data Breach***

Dear [redacted]

We are writing to inform you of a data security incident involving your personal information held by our company, Transak USA LLC. We take privacy and security seriously, and this notice explains the incident, outlines the steps Transak USA LLC and its parent, Transak, Inc., has taken to address it. We also provide guidance on steps you can take to help protect your personal information and an opportunity to enroll in complimentary credit monitoring services.

What Happened

On September 23, 2024, Transak, Inc. received a claim from an unknown malicious individual alleging its unauthorized access and acquisition of Transak data hosted by a third party. Transak initiated an investigation to substantiate the claim. Transak also retained legal counsel and a leading IT forensics expert firm - CrowdStrike - to investigate. As part of the investigation, Transak, Inc. identified the credentials of a single employee that were compromised facilitating access to and acquisition of the data. Transak, Inc. also determined that the access to personal information of Transak USA LLC customers took place between September 1-11, 2024.

What Information Was Involved

The information that may have been impacted includes your first and last name, in combination with your [redacted] No Social Security numbers were involved.

<u>What We Are Doing</u>:

Prior to the incident, both Transak, Inc. and Transak USA LLC had a number of security measures in place. Upon learning of the incident, both companies implemented additional security safeguards. We also retained legal counsel and engaged a leading IT forensic expert firm to investigate the incident. We also have notified law enforcement.

Additionally, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no cost to you. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed "*Steps You Can Take to Help Protect Your Information*."

What You Can Do

As a general matter, it is important to be vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, you should promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, as well as credit monitoring enrollment instructions.

For More Information

Should you have any questions or concerns, please contact our dedicated assistance line at 1-833-799-4043, 8:00 am to 8:00 pm EST, Monday through Friday, excluding major U.S. holidays. Please know that the security of your information is of the utmost importance to us. We remain committed to safeguarding the trust you've placed in us and are deeply grateful for your continued support during this time.

Sincerely,

Transak USA LLC

Enclosure: *Steps You Can Take to Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

To enroll in Credit Monitoring services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts and Credit Reports:

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors.

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

Fraud Alerts:

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Credit Freeze:

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 1-202-727-3400; and oag.dc.gov.

For Iowa residents, the Iowa Attorney General may be contacted at 1305 E. Walnut Street, Des Moise, IA 50419; 1-515-281-5164; and iowaattorneygeneral.gov.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St, Paul Place, Baltimore, MD 21202; 1-410-576-6300; and marylandattorneygeneral.gov.

For Massachusetts residents, the Massachusetts Attorney General may be contacted at 1 Ashburton Place, 20th Floor, Boston, MA 02108; 1-617-727-8400 or 1-617-727-2200; and www.mass.gov/orgs/office-of-the-attorney-general.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and https://doj.state.or.us/consumer-protection/.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. 71 Rhode Island residents had their data impacted by this incident.