

Kennedys

By Email

Attorney General Anthony Brown
Attn: Security Breach Notification
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

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
April 15, 2024

Dear Attorney General Brown:

Our office writes on behalf of our client SMRT Architects & Engineers to provide notice for a data breach impacting the personally identifiable information of one Maryland resident.

On December 3, 2023, SMRT learned that an actor gained unauthorized access to its systems and obtained certain employment records. The actor ultimately published the data on December 19, 2023. It is believed that the actor was the group operating under the moniker “.Play.” SMRT was first alerted of the unauthorized access through its early detection response (EDR) tools. Upon discovery, SMRT took immediate action to secure its systems, which included taking their systems offline. SMRT also retained our office and forensic specialists (through our office) to assist in determining the nature and scope of the incident.

The investigation determined that the unauthorized actor gained access to a SMRT system on December 3, 2023 through the company’s VPN. The exact means was unable to be determined. The personally identifiable information impacted that was impacted for Maryland resident was name and social security number. SMRT is providing written notice to the individuals whose data was impacted, and has offered credit monitoring services through TransUnion. A sample of the notice letter is enclosed. TransUnion has the template and currently is in the process of inserting the appropriate instructions for the credit monitoring and data elements identified per person for mailing. We anticipate the letter will go out soon.

SMRT has since implemented multi-factor authentication across its systems, where feasible. SMRT possess tools to encrypt sensitive data in transit, and with the addition of data at rest encryption as a newly implemented safeguard. SMRT also has a comprehensive data security program in place. SMRT is reviewing and assessing that program, and updating its data security policies and procedures, as appropriate. SMRT is also in the process of looking into further employee IT security training.

Kennedys is a trading name of Kennedys CMK LLP. Kennedys Law LLP, a UK Limited Liability Partnership, is a partner of Kennedys CMK LLP

Kennedys offices, associations and cooperations: Argentina, Australia, Belgium, Bermuda, Brazil, Canada, Chile, China, Colombia, Denmark, Dominican Republic, England and Wales, France, Guatemala, Hong Kong, India, Ireland, Israel, Italy, Mexico, New Zealand, Northern Ireland, Norway, Oman, Pakistan, Panama, Peru, Poland, Portugal, Puerto Rico, Russian Federation, Scotland, Singapore, Spain, Sweden, Thailand, United Arab Emirates, United States of America.

Attorney General Anthony Brown
Office of the Attorney General

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

Enclosure

cc: Ashley Pusey, Esquire



[General US Notice Letter]

SMRT Architects and Engineers
75 Washington Avenue
Suite 3A
Portland, Maine 04101

<<Name>>

<<Address 1>>

<<Address 2>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

NOTICE OF DATA BREACH

Dear <<Name>>:

We are writing to inform you of a data security incident experienced by our company that may have involved your information as described below. We take the privacy and security of all information very seriously and are providing information about the incident and steps you can take to help protect your information.

What Happened: On December 3, 2023, we learned of an unauthorized access to one of our systems that included certain employment records. Upon discovery, we took immediate action to secure our systems and to address and investigate the incident, which included engaging outside forensic specialists to assist with determining the nature and scope of the incident. After a thorough investigation, we learned that the unauthorized actor gained access to one of our systems on December 3, 2023 and acquired certain personal data. As part of the investigation, a thorough review of the system's contents was performed to determine the type of information contained within our files and to whom that information related. This process included working to confirm contact information in order to provide you with this notice.

What Information Was Involved: The types of information contained within the affected data includes your first and last name, in combination with the following data element(s): **person's data elements inserted by TransUnion**.

What We Are Doing: Upon learning of this incident, we immediately took steps to contain the event and undertook a thorough investigation with legal counsel and forensic specialists. Additionally, we are offering you complimentary 12-month credit monitoring and identity protection services through TransUnion at no cost to you and out of an abundance of caution. 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: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please 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 which can be reached at _____ [Toll Free Number inserted by TransUnion], Monday through Friday, excluding major U.S. holidays. Additional information may also be found at <https://www.transunion.com/>. Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

Dennis Morin
Director of Operations

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



STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Insert Credit Monitoring Product Info [inserted by TransUnion].

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.

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.

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 D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

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. There is 1 Rhode Island resident impacted by this incident.



SMRT Architects and Engineers
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
«Keycode»

«firstName» «lastName»
«Address1» «Address2»
«City», «State» «PostalCode»

Date

NOTICE OF DATA BREACH

Dear «FirstName» «LastName»:

We are writing to inform you of a data security incident experienced by our company that may have involved your information as described below. We take the privacy and security of all information very seriously and are providing information about the incident and steps you can take to help protect your information.

What Happened: On December 3, 2023, we learned of an unauthorized access to one of our systems that included certain employment records. Upon discovery, we took immediate action to secure our systems and to address and investigate the incident, which included engaging legal counsel and forensic specialists to assist with determining the nature and scope of the incident. After a thorough investigation, we learned that the unauthorized actor gained access to one of our systems on December 3, 2023 and acquired certain personal data. As part of the investigation, a thorough review of the system's contents was performed to determine the type of information contained within our files and to whom that information related. This process included working to confirm contact information in order to provide you with this notice.

What Information Was Involved: The types of information contained within the affected data includes your first and last name, in combination with the following data element(s): <<exposed data elements>>.

What We Are Doing: Upon learning of this incident, we immediately took steps to contain the event and undertook a thorough investigation with legal counsel and forensic specialists. Additionally, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for <<service length>> 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: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please 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 which can be reached at 1-800-405-6108 from 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding major U.S. holidays. Additional information may also be found at <https://www.transunion.com/>. Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

Dennis Morin
Director of Operations

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 <<URL>> and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE>. 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.

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.

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	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert 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
---	--	---

TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	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 D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

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. There is 1 Rhode Island resident impacted by this incident.