

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

June 28, 2022

Sent via USPS

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Dear Attorney General Frosh:

We represent Smith, Gambrell & Russell, LLP ("SGR") with respect to a data security incident involving personal information as described below. SGR is notifying you of this incident on behalf of Government Employees Insurance Company, which is the owner of the impacted data described herein.

1. Nature of security incident.

On August 9, 2021, SGR learned that documents may have been taken from its information technology ("IT") systems by an unauthorized person. SGR immediately implemented its incident response protocols, contacted law enforcement, and hired external computer forensic specialists and other consultants to address the incident and to investigate what occurred and what data may have been impacted. The investigators identified documents that may have been taken from one server in its environment. A separate vendor was then hired to review the potentially impacted documents to identify any personal information contained within them. This review was partially completed on May 17, 2022, at which point SGR learned that some information belonging to Government Employees Insurance Company (the "Company") was present in the impacted documents. SGR provided the Company with the final data file for its review and cooperated with the Company's investigation into the scope and impact of the incident. SGR then worked with the Company to prepare notification letters, arrange for mailing, and arrange for impacted individuals to receive credit monitoring and identity restoration services.

2. Number of residents affected.

Seven (7) Maryland residents may have been affected and were notified of the incident. For individuals associated with the Company, a letter was sent to the potentially affected individuals on June 28, 2022, via regular mail (a copy of the form notification letter is enclosed). Impacted information may include names, and some combination of the following: Social Security number, driver's license number, government ID, medical information such as treatment, diagnosis, and/or medical history.

3. Steps taken in response to the incident.

Since this incident, SGR deployed enhanced endpoint monitoring software for all endpoints, performed a global password reset for all users, emphasized additional security training and awareness, and implemented additional security controls. SGR is also working with a cybersecurity firm to assess its information security controls and is committed to continually improving its security posture. Additionally, potentially affected individuals were offered 12 months of credit monitoring and identity protection services through IDX at no cost.

4. Contact information.

SGR takes very seriously the need to protect the privacy and security of all information in its care. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL



Melissa K. Ventrone
Member

cc: Mariah Leffingwell – mleffingwell@clarkhill.com
Brett Lockwood – blockwood@sgrlaw.com



Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-423-2985

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

June 28, 2022

<<Variable Text 2: NOTICE OF DATA SECURITY INCIDENT / NOTICE OF DATA BREACH>>

Dear <<FIRST NAME>> <<LAST NAME>>,

This is to let you know about a data security incident that may have impacted your personal information. Smith, Gambrell & Russell, LLP ("SGR") is a law firm that provides services to primarily corporate clients and, in that capacity, may have been provided with your information in the performance of services for the Government Employees Insurance Companies (collectively the "Company"). We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you do so.

What Happened?

On August 9, 2021 we learned that some documents may have been taken from a part of our information technology ("IT") systems by an unauthorized person. We immediately implemented our incident response protocols, contacted law enforcement, and hired external computer forensic specialists and other consultants to address the incident and to investigate what occurred and what data may have been impacted. The investigators identified a number of documents that may have been taken. We then hired a vendor to review the potentially impacted documents to identify any personal information contained within them. This review was completed on May 17, 2022, at which point we learned that some of your information may have been in the impacted documents. However, we have no indication that any of your information was misused and this letter is being provided out of an abundance of caution.

What Information Was Involved?

From our review, it appears that the personal information of yours contained in the impacted documents may have included your name, driver's license number, and for some individuals, their address.

What We Are Doing

We want to assure you that we have taken, and continue to take, steps to prevent a similar incident from happening in the future. Since the incident, we deployed enhanced endpoint monitoring software on our computers and servers, performed a global password reset for all users, provided additional security training, and implemented several other security controls. We also notified and are cooperating with law enforcement.

In addition, we are offering identity theft protection services through IDX, a leading data breach and recovery services provider, at no charge to you. IDX identity protection services include: <<Variable Text 1: twelve (12) / twenty-four (24)>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-423-2985 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is September 28, 2022. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. The information below also contains some state notices that may be applicable to you depending on the state in which you reside.

For More Information

If you have any questions or concerns, please call 1-833-423-2985 Monday through Friday from 9 am - 9 pm Eastern Time. Please be assured that we and the Company take very seriously the need to protect the privacy and security of all information in our respective care, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Smith, Gambrell + Russell, LLP

Smith, Gambrell & Russell, LLP



Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at **1-833-423-2985** to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Some state notices that may be applicable to you depending on the state in which you reside are also noted below.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. You should report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed regarding this incident. Four Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

August 8, 2022

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202



Who Whom It May Concern:

We represent Smith Gambrell & Russell, LLP ("SGR") as outside counsel with respect to a data security incident, of which you were previously notified on June 28, 2022. SGR is notifying your office of this incident on behalf of its clients, who are the owners of the impacted data. We are writing to inform you that notice was also provided to impacted individuals at the request of SGR clients listed in Exhibit A. The number of Maryland residents impacted are identified in Exhibit A as well. Residents were notified via regular mail on August 8th and 9th, 2022, and a copy of the template letter is attached as Exhibit B. Please contact me if you have any questions.

Sincerely,
CLARK HILL

A handwritten signature in black ink, appearing to read 'M K Ventrone'.

Melissa K. Ventrone
Member

cc: Mariah Leffingwell – mleffingwell@clarkhill.com
Brett Lockwood – blockwood@sgrlaw.com

Exhibit A

Company Name	Number of Individuals
Sunbelt Rentals, Inc.	19
Modis, Inc.	1
Valmet Corporation	1

Exhibit B



Return to IDX
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-423-2985
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>><<Address2>>
<<City>>, <<State>> <<ZIP>>

August 9, 2022

NOTICE OF DATA <<BREACH / SECURITY INCIDENT>>

Dear <<First Name>> <<Last Name>>,

This is to let you know about a data security incident that may have impacted your personal information. Smith, Gambrell & Russell, LLP ("SGR") is a law firm that provides services to clients and, in that capacity, may have been provided with your information in the performance of services for <<Variable Text>>. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you do so.

What Happened?

On August 9, 2021 we learned that some documents may have been taken from a part of our information technology systems by an unauthorized person. We immediately implemented our incident response protocols, contacted law enforcement, and hired external computer forensic specialists and other consultants to address the incident and to investigate what occurred and what data may have been impacted. The investigators identified a number of documents that may have been taken. We then hired a vendor to review the potentially impacted documents to identify any personal information contained within them. This review was only recently completed, at which point we learned that some of your information may have been in the impacted documents. However, we have no indication that any of your information was actually misused and this notice is being provided out of an abundance of caution.

What Information Was Involved?

From our review, it appears that the personal information of yours contained in the impacted documents may have included your name, <<Variable Text>>.

What We Are Doing

We want to assure you that we have taken, and continue to take, steps to prevent a similar incident from happening in the future. Since the incident, we deployed enhanced endpoint monitoring software on our computers and servers, performed a global password reset for all users, provided additional security training, and implemented several other security controls. We also notified and are cooperating with law enforcement.

In addition, we are offering identity theft protection services through IDX, a leading data breach and recovery services provider, at no charge to you. IDX identity protection services include: twelve (12) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-423-2985 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is November 9, 2022. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. The information below also contains some state notices that may be applicable to you depending on the state in which you reside.

For More Information

If you have any questions or concerns, please call 1-833-423-2985 Monday through Friday from 9 am - 9 pm Eastern Time. Please be assured that we take very seriously the need to protect the privacy and security of all information in our respective care, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Smith, Gambrell & Russell, LLP

Smith, Gambrell & Russell, LLP



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-423-2985 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Some state notices that may be applicable to you depending on the state in which you reside are also noted below.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. You should report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed regarding this incident. [XX] Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email:mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

September 28, 2022

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Frosh:

We represent Smith Gambrell & Russell, LLP (“SGR”) as outside counsel with respect to a data security incident, of which we originally notified you on June 28, 2022. SGR is notifying your office of this incident on behalf of its clients, who are the owners of the impacted data. We are writing to inform you that notice was also provided to impacted individuals directly on behalf of SGR. A total of twenty-six (26) Maryland residents were notified on behalf of SGR via regular mail on September 28, 2022. A copy of the template letter is attached as Exhibit A. Please contact me if you have any questions.

Sincerely,
CLARK HILL

A handwritten signature in black ink, appearing to read 'M K Ventrone'.

Melissa K. Ventrone
Member

cc: Mariah Leffingwell – mleffingwell@clarkhill.com
Brett Lockwood – blockwood@sgrlaw.com



Return to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-423-2985

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>

<<ADDRESS1>>

<<ADDRESS2>>

<<CITY>>, <<STATE>> <<ZIP>>

<<Country>>

September 28, 2022

NOTICE OF DATA <<SECURITY INCIDENT / BREACH>>

Dear <<FIRST NAME>> <<LAST NAME>>,

This is to let you know about a data security incident that involved your personal information. Smith, Gambrell & Russell, LLP (“SGR”) is a law firm that provides services to primarily corporate clients and, in that capacity, was provided with your information in connection with the performance of our client services. We sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you do so.

What Happened?

On August 9, 2021 we learned that some documents may have been taken from a part of our information technology systems by an unauthorized person. We immediately implemented our incident response protocols, contacted law enforcement, and hired external computer forensic specialists and other consultants to address the incident and to investigate what occurred and what data may have been impacted. The investigators identified a number of documents that may have been taken. We then hired a vendor to review the potentially impacted documents to identify any personal information contained within them. This review was only recently completed, at which point we learned that some of your information may have been in the impacted documents. However, we have no indication that any of your information was actually misused and this notice is being provided out of an abundance of caution.

What Information Was Involved?

From our review, it appears that the personal information of yours contained in the impacted documents may have included the following: name, <<Variable Text 1>>.

What We Are Doing

We want to assure you that we have taken, and continue to take, steps to prevent a similar incident from happening in the future. Since the incident, we deployed enhanced endpoint monitoring software on our computers and servers, performed a global password reset for all users, provided additional security training, and implemented several other security controls. We also notified and are cooperating with law enforcement.

In addition, we are offering identity theft protection services through IDX, a leading data breach and recovery services provider, at no charge to you. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

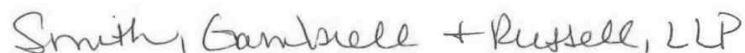
It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-423-2985 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is December 28, 2022. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. The information below also contains some state notices that may be applicable to you depending on the state in which you reside.

For More Information

If you have any questions or concerns, please call 1-833-423-2985 Monday through Friday from 9 am - 9 pm Eastern Time. Please be assured that we take very seriously the need to protect the privacy and security of all information in our respective care, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

A handwritten signature in black ink that reads "Smith, Gambrell & Russell, LLP". The signature is written in a cursive, slightly slanted style.

Smith, Gambrell & Russell, LLP



Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-423-2985 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Some state notices that may be applicable to you depending on the state in which you reside are also noted below.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. You should report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed regarding this incident. 7 Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

December 13, 2022

VIA ELECTRONIC MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Brian E. Frosh:

We represent Smith Gambrell & Russell, LLP (“SGR”) as outside counsel with respect to a data security incident, of which we originally notified you on June 28, 2022, and provided updates on August 8, 2022 and September 28, 2022. SGR is notifying your office of this incident on behalf of its clients, who are the owners of the impacted data. We are writing to inform you that notice was also provided to impacted individuals at the request of SGR’s client, Aaron’s, LLC. An additional 797 Maryland residents were notified of the incident via regular mail on December 13, 2022. A copy of the template letter is attached as Exhibit A. Please contact me if you have any questions.

Sincerely,
CLARK HILL

A handwritten signature in dark ink, appearing to read 'M K Ventrone'.

Melissa K. Ventrone
Member

cc: Mariah Leffingwell – mleffingwell@clarkhill.com
Brett Lockwood – blockwood@sgrlaw.com



Return to IDX
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-423-2985
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

December 13, 2022

<<NOTICE OF DATA BREACH / Notice of Data Security Incident>>

Dear <<First Name>> <<Last Name>>,

This is to let you know about a data security incident that may have impacted your personal information. Smith, Gambrell & Russell, LLP (“SGR”) is a law firm that provides services to primarily corporate clients and, in that capacity, may have been provided with your information in the performance of services for Aaron’s, LLC (the “Company”). We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you do so.

What Happened?

On August 9, 2021 we learned that some documents may have been taken from a part of our information technology systems by an unauthorized person. We immediately implemented our incident response protocols, contacted law enforcement, and hired external computer forensic specialists and other consultants to address the incident and to investigate what occurred and what data may have been impacted. The investigators identified a number of documents that may have been taken during the period July 19 through July 28, 2021. We then hired a vendor to review the potentially impacted documents to identify any personal information contained within them. We completed this review, and then notified Aaron’s of the incident on October 25, 2022. Thereafter, we provided Aaron’s with access to the potentially impacted documents for their review, and based on their review, which was completed on November 16, 2022, they determined that some of your personal information was contained in the potentially impacted documents. However, we have no indication that any of your information was actually misused and this notice is being provided out of an abundance of caution.

What Information Was Involved?

From the review, it appears that the personal information of yours contained in the impacted documents may have included your name, <<Variable Text>>.

What We Are Doing

We want to assure you that we have taken, and continue to take, steps to prevent a similar incident from happening in the future. Since the incident, we deployed enhanced endpoint monitoring software on our computers and servers, performed a global password reset for all users, provided additional security training, and implemented several other security controls. We also notified and are cooperating with law enforcement.

In addition, we are offering identity theft protection services through IDX, a leading data breach and recovery services provider, at no charge to you. IDX identity protection services include: twenty-four (24) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

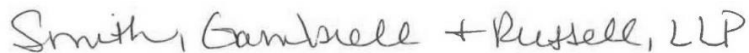
It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-423-2985 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is March 13, 2023. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. The information below also contains some state notices that may be applicable to you depending on the state in which you reside.

For More Information

If you have any questions or concerns, please call 1-833-423-2985 Monday through Friday from 9 am - 9 pm Eastern Time. Please be assured that we and the Company take very seriously the need to protect the privacy and security of all information in our respective care, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Smith, Gambrell + Russell, LLP".

Smith, Gambrell & Russell, LLP



Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-833-423-2985 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Some state notices that may be applicable to you depending on the state in which you reside are also noted below.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. You should report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed regarding this incident. 106 Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

December 13, 2022

VIA ELECTRONIC MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Dear Attorney General Brian E. Frosh:

We represent Smith Gambrell & Russell, LLP (“SGR”) as outside counsel with respect to a data security incident, of which we originally notified you on June 28, 2022, and provided updates on August 8, 2022 and September 28, 2022. SGR is notifying your office of this incident on behalf of its clients, who are the owners of the impacted data. We are writing to inform you that notice was also provided to impacted individuals at the request of SGR’s client, Aaron’s, LLC. An additional 797 Maryland residents were notified of the incident via regular mail on December 13, 2022. A copy of the template letter is attached as Exhibit A. Please contact me if you have any questions.

Sincerely,
CLARK HILL

A handwritten signature in dark ink, appearing to read 'M K Ventrone', with a horizontal line extending to the right.

Melissa K. Ventrone
Member

cc: Mariah Leffingwell – mleffingwell@clarkhill.com
Brett Lockwood – blockwood@sgrlaw.com



Return to IDX
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-423-2985
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

December 13, 2022

<<NOTICE OF DATA BREACH / Notice of Data Security Incident>>

Dear <<First Name>> <<Last Name>>,

This is to let you know about a data security incident that may have impacted your personal information. Smith, Gambrell & Russell, LLP ("SGR") is a law firm that provides services to primarily corporate clients and, in that capacity, may have been provided with your information in the performance of services for Aaron's, LLC (the "Company"). We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this incident may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you do so.

What Happened?

On August 9, 2021 we learned that some documents may have been taken from a part of our information technology systems by an unauthorized person. We immediately implemented our incident response protocols, contacted law enforcement, and hired external computer forensic specialists and other consultants to address the incident and to investigate what occurred and what data may have been impacted. The investigators identified a number of documents that may have been taken during the period July 19 through July 28, 2021. We then hired a vendor to review the potentially impacted documents to identify any personal information contained within them. We completed this review, and then notified Aaron's of the incident on October 25, 2022. Thereafter, we provided Aaron's with access to the potentially impacted documents for their review, and based on their review, which was completed on November 16, 2022, they determined that some of your personal information was contained in the potentially impacted documents. However, we have no indication that any of your information was actually misused and this notice is being provided out of an abundance of caution.

What Information Was Involved?

From the review, it appears that the personal information of yours contained in the impacted documents may have included your name, <<Variable Text>>.

What We Are Doing

We want to assure you that we have taken, and continue to take, steps to prevent a similar incident from happening in the future. Since the incident, we deployed enhanced endpoint monitoring software on our computers and servers, performed a global password reset for all users, provided additional security training, and implemented several other security controls. We also notified and are cooperating with law enforcement.

In addition, we are offering identity theft protection services through IDX, a leading data breach and recovery services provider, at no charge to you. IDX identity protection services include: twenty-four (24) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

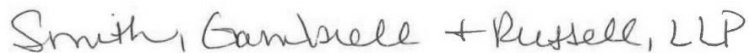
It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-423-2985 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is March 13, 2023. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Additional information about protecting your identity is included in this letter, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. The information below also contains some state notices that may be applicable to you depending on the state in which you reside.

For More Information

If you have any questions or concerns, please call 1-833-423-2985 Monday through Friday from 9 am - 9 pm Eastern Time. Please be assured that we and the Company take very seriously the need to protect the privacy and security of all information in our respective care, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Smith, Gambrell + Russell, LLP".

Smith, Gambrell & Russell, LLP



Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-833-423-2985 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Some state notices that may be applicable to you depending on the state in which you reside are also noted below.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: You should report any suspected identity theft to law enforcement or to the Iowa Attorney General, Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. You should report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed regarding this incident. 106 Rhode Island residents were notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



January 30, 2023

Anjali C Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Email: IDTheft@oag.state.md.us

Attorney General Anthony G. Brown

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

Re: Supplemental Notice of Data Security Incident
Client: Homeschool Legal Defense Association
File No.: 15991.01190

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman & Dicker LLP (“Wilson Elser”) represents Homeschool Legal Defense Association (“HSLDA”), headquartered in Purcellville, Virginia with respect to a recent data security incident. HSLDA is a non-profit organization providing non-legal services to families who homeschool their children. HSLDA takes this matter very seriously and is taking measures to remediate the incident and has provides notice to potentially affected individuals.

This letter will serve to supplement our prior notice with regards to this incident submitted to your office on March 4, 2022, and inform you of additional information regarding the nature of the incident, the number of additional Maryland residents being notified, and further steps that HSLDA has taken in response to the incident.

1. Nature of the incident.

On February 2, 2022, HSLDA was notified by a third-party service provider of suspicious activity involving its payroll management system. Immediately upon notification, HSLDA took steps to mitigate the impact of the incident by shutting down access to the payroll system, changing passwords, and engaging third party experts to assist in remediation steps. Additionally, HSLDA commenced an investigation to determine the nature and scope of the incident. The investigation revealed that an unauthorized party gained access to HSLDA’s payroll system using compromised credentials. While the investigation was unable to confirm the specific employee information that may have been accessed, HSLDA provided notice to all employees, regardless of whether their information was confirmed to be subject to unauthorized access or acquisition.

Upon completing the first round of notification, HSLDA subsequently engaged a third-party data mining vendor to conduct a further review of the information that may have been involved in the incident. Upon completion of its investigation, HSLDA discovered that additional individuals may have been impacted by the incident. HSLDA has since worked to identify the individuals whose information may have been involved in the incident. On January 19, 2023, HSLDA provided a second round of notice to the additional

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

266884436v.1

individuals whose information was affected as a result of the incident.

2. Number of Maryland residents affected.

HSLDA discovered that an additional twenty-five (25) resident of Maryland were impacted by this incident. Notification letters were sent to these individuals on January 19, 2023. A sample notice letter that was sent to the impacted individuals is included as **Exhibit A**.

3. Steps taken.

HSLDA takes the security of personal information in its control very seriously, and has taken steps to prevent a similar event from occurring in the future, including but not limited to: strengthened internal password policy by increasing complexity and enhanced secure login authentication procedures for third party service provider accounts.

Further, HSLDA has provided the individuals whose PII was potentially accessed by an unauthorized individual with twelve (12) months of unlimited access to their Equifax credit report and credit score as well as a daily credit monitoring service that will notify the individual if there are any critical changes to their credit file at Equifax. The services provided also include access to an identity restoration program that provides assistance in the event that an individual's identity is compromised to help them restore their identity and up to \$1,000,000 in identity theft insurance.

4. Contact information.

HSLDA remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

<<Variable Header>>

Dear <<Name 1>>:

We are writing to inform you of a data security incident which affected Homeschool Legal Defense Association (“HSLDA”), a non-profit organization dedicated to assisting families with homeschooling services located in Purcellville, Virginia. The data security incident may have impacted some of your personal data. This letter contains information about the incident and information about how to protect your personal information going forward. HSLDA considers the protection of sensitive information a top priority, and sincerely apologizes for any inconvenience as a result of the incident. At this time, we have no indication that your information has been misused.

What Happened

On February 2, 2022, HSLDA was notified by one of our third-party service providers of suspicious activity involving our payroll management system. Immediately upon notification, we took steps to mitigate further harm by shutting down access to the payroll system, changing passwords, and engaging third party experts to assist in remediation steps. Additionally, HSLDA commenced an investigation to determine the nature and scope of the incident. The investigation revealed that an unauthorized party gained access to HSLDA’s payroll system using compromised credentials. While the investigation was unable to confirm the specific employee information that may have been accessed, HSLDA provided notice to all employees, regardless of whether their information was confirmed to be subject to unauthorized access or acquisition.

Upon completing the first round of notification, HSLDA engaged a third-party data mining vendor to conduct a further review of the information that may have been involved in the incident. Upon completion of its investigation, HSLDA discovered that additional individuals may have been impacted by the incident. HSLDA has since worked to provide notice to all individuals whose information may have been impacted as result of the incident.

What Information Was Involved

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the unauthorized party may have had access to <<Affected Data>>.

What We Are Doing

The security and privacy of your personal information contained within HSLDA systems is a top priority, and HSLDA is taking additional measures to protect this information. Since the incident, HSLDA has continued to strengthen its security posture by adding security controls, including strengthening its internal password policy by increasing complexity and enhancing secure login authentication procedures for third party service provider accounts.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (1-Bureau Credit Watch Gold) for twelve (12) months provided by Equifax, one of the three nationwide credit reporting companies.

You can sign up for the credit monitoring service anytime between now and **April 30th 2023**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with Equifax, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain twelve (12) months of unlimited access to your Equifax credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at Equifax, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

How Do I Enroll for the Free Services?

To enroll in this service, go to the Equifax website at www.equifax.com/activate and in the space referenced as “Enter Activation Code”, enter the following Activation Code <<Activation Code>> and follow the steps to receive your credit monitoring service. Please see more information regarding the enrollment process at the end of this letter.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Important Information*, to learn more about how to protect against the possibility of information misuse.

The protection of your personal information is a top priority and we sincerely regret any concern or inconvenience this matter may cause. If you have any questions, please do not hesitate to call **1-855-962-3266** Monday through Friday, between 9:00 AM and 9:00 PM, Eastern Time.

Sincerely,



Charles L. Hurst
VP of Administration
Homeschool Legal Defense Association

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fair Credit Reporting Act: You are also advised that you may have additional rights under the federal Fair Credit Reporting Act.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for

your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
(800)-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
(888)-397-3742

www.experian.com/freeze

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
(800)-680-7289

freeze.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.



Hogan Lovells US LLP
390 Madison Avenue
New York, NY 10017
T +1 212 918 3000
F +1 212 918 3100
www.hoganlovells.com

February 1, 2023

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

By Email

To Whom It May Concern:

I am writing on behalf of Diligent Corporation ("Diligent" or "Company") to provide you with an update regarding a previously reported cybersecurity event.

Subsequent to Diligent's initial notification to your office on June 21, 2022, the unauthorized actor posted a set of files that it had acquired on an external site. This enabled the Company to identify additional impacted Maryland residents, as well as additional types of personal information involved in the event. As of the date of this letter, approximately 31 Maryland residents have been identified as impacted. The types of personal information that may have been accessed include: names; dates of birth; email addresses; mailing addresses; phone numbers; usernames with passwords and/or security codes; health/medical information; health insurance information; government identification numbers; financial account numbers; payment card information; and Social Security numbers or taxpayer identification numbers.

Diligent is providing notice by mail to the additional Maryland residents identified as impacted, and a sample copy of such notice is attached. In addition to providing information regarding credit reporting agencies, government resources, security freezes, and fraud alerts, Diligent is offering credit monitoring services for two years through Experian, at no cost to the affected individuals.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

/s/

Peter Marta
Counsel to Diligent Corporation
peter.marta@hoganlovells.com
(212) 918-3528