

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

***CONFIDENTIAL
VIA PORTAL***

Commissioner Mike Kreidler
Office of the Insurance Commissioner
P.O. Box 40255
Olympia, WA 98504-0255

Dear Commissioner Kreidler:

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 Aaron’s, LLC (the “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. SGR notified the Company of the incident on October 25, 2022. Thereafter, SGR provided the Company with access to the potentially impacted documents for their review, and based on their review, which was completed on November 16, 2022, the Company determined that customer personal information was contained in the potentially impacted documents. 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.

Five-hundred sixteen (516) Washington residents associated with the Company were affected. A letter was sent to the potentially affected individuals on December 13, 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.

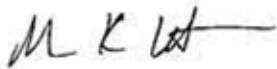
Since this incident, SGR deployed enhanced endpoint monitoring software for all endpoints, performed a global password reset for all users, changed the user's password, emphasized additional security training and awareness, and implemented additional security controls. SGR is also working with a cybersecurity firm to assess its information security controls and is committed to continually improving its security posture. Additionally, potentially affected individuals were offered 24 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 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

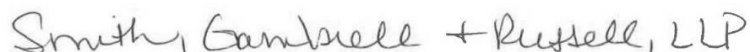
It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 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.



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

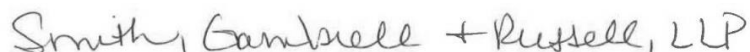
It is always a good idea to review your credit reports, bank account and other financial statements, and immediately contact your financial institution if you identify suspicious activity. We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 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.