

Richard Halm
T (312)985-5564
F (312)985-5952
Email: rhalm@clarkhill.com

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

February 27, 2025

VIA ELECTRONIC MAIL

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

Dear Attorney General Brown:

We represent Service Access & Management, Inc. (“SAM”) with respect to a data security incident involving personal information described below. SAM is a nonprofit organization that provides that provides a number of human services throughout Pennsylvania and New Jersey. For some of the services, SAM is considered a covered entity as defined under the Health Insurance Portability and Accountability Act (“HIPAA”). SAM takes the security of the information in its control seriously and is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

1. Nature of security incident.

On July 5, 2024, SAM discovered suspicious activity on its systems, immediately implemented its incident response protocols, and began an internal investigation. SAM also engaged cybersecurity and data forensic specialists to assist in identifying what happened and whether any sensitive information was potentially affected. This investigation determined that an unauthorized user potentially accessed SAM’s systems and, on September 12, 2024, SAM determined which files were potentially affected. The files then had to be reviewed to determine what, if any, personal information (“PI”) or protected health information (“PHI”) they contained. This review was completed on January 31, 2025. The results of this review then had to be supplemented with additional mailing address for individuals who had none. This was completed on February 18, 2025.

2. Number of residents affected.

A total of seventeen (17) Maryland residents were notified of the incident. One (1) of these individuals had PHI affected and sixteen (16) had PI affected. Affected data elements include names, Social Security numbers and in some cases medical information. A notification letter was

February 27, 2025

Page 2

sent to the potentially affected individuals on February 27, 2025 (a copy of the form notification letters are enclosed as Exhibit A).

3. Steps taken in response to the incident.

Since the incident, SAM has performed an organization-wide credential reset and rebuilt any affected systems. Additionally, potentially affected individuals were offered 12 months of credit monitoring and identity protection services through IDX at no cost.

4. Contact Information

SAM takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at rhalm@clarkhill.com or (312) 985-5564.

Sincerely,
CLARK HILL

A handwritten signature in cursive script that reads "Richard Halm".

Richard Halm

cc: Milea Moye



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

Parent or Guardian of

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

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

<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

February 27, 2025

RE: <<Variable Text 2: Notice of Data Security Incident/Notice of Data Breach>>

Dear Parent or Guardian of <<First Name>> <<Last Name>>:

We are writing to let you know about a data security incident that may have affected your child's personally identifiable information ("PII"). Service Access & Management, Inc. ("SAM") takes the privacy and security of all information of recipients of its services seriously, and sincerely apologizes for any concern or inconvenience this notice may cause you. SAM is a nonprofit organization that provides a number of human services throughout Pennsylvania and New Jersey. SAM may have had your child's data if he or she or a family member received their services. This letter contains information about steps you can take to protect his or her information and resources we are making available to help him or her.

What Happened?

On July 5, 2024, SAM discovered suspicious activity on its network and immediately began an investigation to identify what happened and whether any patient information was potentially affected. SAM also implemented its incident response protocols and engaged third-party forensic experts to assist in the investigation. This investigation determined that an unauthorized user potentially accessed SAM's systems and, on September 12, 2024, SAM determined which files were potentially affected. The files then had to be reviewed to determine what, if any, PII they contained. This review was completed on January 31, 2025, and determined that some of your child's data may have been in the affected systems. SAM takes the privacy and security of data in its possession very seriously, at this time, there is no evidence that your child's data has been misused. However, we are providing you notice out of an abundance of caution.

What Information Was Involved?

From our review it appears that your child's name and the following data elements may have been impacted: <<Variable Text 1: Data Elements>>.

What We Are Doing to Protect Your Child's Information:

We want to assure you that we are taking steps to prevent a similar incident from happening in the future. Since the incident, SAM has performed an organization-wide password reset, notified law enforcement and rebuilt any affected systems.

To help protect your child's identity, we are offering a complimentary <<12/24>> months membership of identity protection services through IDX. IDX identity protection services include CyberScan monitoring, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-877-425-9971 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 May 27, 2025.

Again, at this time, there is no evidence that your child's information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information:

You will find detailed instructions for enrollment on the enclosed document *Additional Recommended Steps to Help Protect Your Minor's Information*. Also, 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.

Please call 1-877-425-9971 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,



Mary Ann Kowalonek
President/CEO
Service Access & Management, Inc.

Additional Recommended Steps to Help Protect Your Minor's Information

1. Website and Enrollment. Scan the QR image or 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. Credit Monitoring Activation. Activate the identity monitoring provided as part of your child's IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have 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 1-877-425-9971 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your minor's identity.

4. Review your minor's 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 minor's 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 your minor falls victim to identity theft, 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 your minor ever experiences 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 your minor has 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 minor's 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 minor's existing accounts. For that reason, placing a fraud alert can protect your minor, but also may delay your minor when they seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351

www.equifax.com/personal/credit-report-services

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

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289

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 minor's credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your minor's personal identifying information will not be able to use that information to open new accounts or borrow money in your minor's 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, your minor 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.

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: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

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.

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 in regard to this incident. There are 0 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft.



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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

February 27, 2025

RE: <<Variable Text 2: Notice of Data Security Incident/Notice of Data Breach>>

Dear <<First Name>> <<Last Name>>:

We are writing to let you know about a data security incident that may have affected your personally identifiable information ("PII"). Service Access & Management, Inc. ("SAM") takes the privacy and security of all information of recipients of its services seriously, and sincerely apologizes for any concern or inconvenience this notice may cause you. SAM is a nonprofit organization that provides a number of human services throughout Pennsylvania and New Jersey. SAM may have had your data if you or a family member received their services. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened?

On July 5, 2024, SAM discovered suspicious activity on its network and immediately began an investigation to identify what happened and whether any personal information was potentially affected. SAM also implemented its incident response protocols and engaged third-party forensic experts to assist in the investigation. This investigation determined that an unauthorized user potentially accessed SAM's systems and, on September 12, 2024, SAM determined which files were potentially affected. These files then had to be reviewed to determine what, if any, PII they contained. This review was completed on January 31, 2025, and determined that some of your data may have been in the affected systems. SAM takes the privacy and security of data in its possession very seriously, at this time, there is no evidence that your data has been misused. However, we are providing you notice out of an abundance of caution.

What Information Was Involved?

From our review it appears that your name and the following data elements may have been impacted: <<Variable Text 1: Data Elements>>.

What We Are Doing to Protect Your Information:

We want to assure you that we are taking steps to prevent a similar incident from happening in the future. Since the incident, SAM has performed an organization-wide password reset, notified law enforcement and rebuilt any affected systems.

To help protect your identity, we are offering a complimentary <<12/24>> months membership of credit monitoring and identity protection services through IDX. IDX identity protection services include CyberScan monitoring, 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:

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-877-425-9971 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 May 27, 2025.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information:

You will find detailed instructions for enrollment on the enclosed document *Additional Recommended Steps to Help Protect Your Information*. Also, 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.

Please call 1-877-425-9971 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "Mary Ann Kowalonek". The signature is fluid and cursive, with the first name "Mary" and last name "Kowalonek" clearly distinguishable.

Mary Ann Kowalonek
President/CEO
Service Access & Management, Inc.

Additional Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or 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. Credit Monitoring Activation. 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 1-877-425-9971 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, 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
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351

www.equifax.com/personal/credit-report-services

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

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289

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.

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: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

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.

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 in regard to this incident. There are 0 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft.



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

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

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

February 27, 2025

RE: <<Variable Text 2: Notice of Data Security Incident/Notice of Data Breach>>

Dear <<First Name>> <<Last Name>>:

We are writing to let you know about a data security incident that may have affected your protected health information ("PHI"). Service Access & Management, Inc. ("SAM") takes the privacy and security of all patient information seriously, and sincerely apologizes for any concern or inconvenience this notice may cause you. SAM is a nonprofit organization that provides a number of human services throughout Pennsylvania and New Jersey. SAM may have had your data if you received their services. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened?

On July 5, 2024, SAM discovered suspicious activity on its network and immediately began an investigation to identify what happened and whether any patient information was potentially affected. SAM also implemented its incident response protocols and engaged third-party forensic experts to assist in the investigation. This investigation determined that an unauthorized user potentially accessed SAM's systems and, on September 12, 2024, SAM determined which files were potentially affected. The files then had to be reviewed to determine what, if any, PHI they contained. This review was completed on January 31, 2025, and determined that some of your data may have been in the affected systems. SAM takes the privacy and security of data in its possession very seriously, at this time, there is no evidence that your data has been misused. However, we are providing you notice out of an abundance of caution.

What Information Was Involved?

From our review it appears that your name and the following data elements may have been impacted: <<Variable Text 1: Data Elements>>.

What We Are Doing to Protect Your Information:

We want to assure you that we are taking steps to prevent a similar incident from happening in the future. Since the incident, SAM has performed an organization-wide password reset, notified law enforcement and rebuilt any affected systems.

To help protect your identity, we are offering a complimentary <<12/24>> months membership of credit monitoring and identity protection services through IDX. IDX identity protection services include CyberScan monitoring, 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:

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-877-425-9971 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 May 27, 2025.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information:

You will find detailed instructions for enrollment on the enclosed document *Additional Recommended Steps to Help Protect Your Information*. Also, 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.

Please call 1-877-425-9971 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read "Mary Ann Kowalonek". The signature is fluid and cursive, with the first name "Mary" and last name "Kowalonek" clearly distinguishable.

Mary Ann Kowalonek
President/CEO
Service Access & Management, Inc.

Additional Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or 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. Credit Monitoring Activation. 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 1-877-425-9971 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, 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
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351

www.equifax.com/personal/credit-report-services

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

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289

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.

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: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

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.

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 in regard to this incident. There are 0 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft.