

Christopher L. Ingram
Direct Dial (614) 464-5480
Direct Fax (614) 464-5480
Email clingram@vorys.com

August 3, 2023

VIA E-MAIL

Office of the Maryland Attorney General
IDTheft@oag.state.md.us

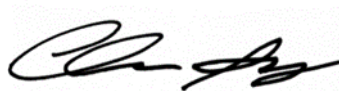
To Office of the Maryland Attorney General:

We write to inform you of a recent data security incident involving Ada Technologies Inc. ("Ada Technologies"), located at 805 E North Ave #1809, Ada, OH 45810. Ada Technologies learned that certain systems on its network were encrypted on or about June 13, 2023. An investigation was immediately initiated. Ada Technologies was unable to confirm whether any specific personal information was accessed or acquired. Out of an abundance of caution, Ada Technologies will be notifying one Maryland resident whose information was believed to have been saved on a server that was encrypted as a result of this incident.

More information regarding this matter is described in the enclosed sample notification letter. The notification letter is being printed now and will be sent via postal mail directly to the affected Maryland residents on or about August 4, 2023.

Please contact us with any questions or concerns.

Very truly yours,



Christopher L. Ingram

Enclosure



Return Mail Processing
PO Box 999
Suwanee, GA 30024

10 1 2365 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



August 4, 2023

NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to inform you of a recent incident involving unauthorized access to our computer network. While we have no indication that your personal information has been accessed or misused, some of your personal information was saved on servers impacted by the incident. We are writing to make you aware of our current understanding of what happened, measures that have been taken, and to provide you with some steps you can take to protect your personal information.

What happened?

On June 13, 2023, we learned that systems on our network were encrypted. We immediately initiated an investigation and retained a leading computer security firm. During the course of the investigation, we learned that there was unauthorized access to systems on the network and that the intruder encrypted files on those systems. We were unable to confirm whether any specific personal information was accessed or acquired. Out of an abundance of caution, we are notifying you of the incident.

What information was involved?

While we were unable to determine whether any personal information was accessed or acquired, the following information may have been saved on a server impacted by the incident: first name, last name, social security number, date of birth, driver's license number, and health insurance information. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

What we are doing.

As soon as we learned of this situation, we immediately launched an investigation and retained a leading computer security firm. We took steps to block unauthorized users from connecting to our network and to prevent future security breaches. Based on our current investigation, we believe this incident was limited to this one event.

What you can do.

Although we do not have any evidence that your information has been misused, we recommend that you review the information provided in the enclosed "Further Information and Steps You Can Take." The enclosure identifies some steps you can take to guard against the misuse of your personal information. Never provide personal information in a response to an electronic communication about a data security incident. Additionally, out of an abundance of caution, we are providing identity theft protection services through a one-year membership of Experian's® IdentityWorksSM at no cost to you. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: October 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 855-797-1033 by **October 31, 2023**, from Monday through Friday 8 am – 10 pm CST, or Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Be prepared to provide B099974 as proof of eligibility for the identity restoration services by Experian.

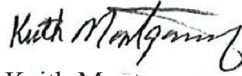
For more information.

We sincerely regret and apologize for any inconvenience this may cause you. Please do not hesitate to contact us at 855-797-1033 if you have any questions or concerns.

Sincerely,



Noriyuki Suzuki, President



Keith Montgomery, Vice President

Enclosure: Further Information and Steps You Can Take

Further Information and Steps You Can Take

Additional details regarding the One-Year Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1M Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 855-797-1033. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Filing a Police Report for Suspicious Activity

We encourage you to remain vigilant of identity theft or fraud. You should review account statements, explanation of benefits, and credit reports and report any suspicious activity or suspected identity theft. You have the right to file a police report if you experience identity theft or fraud. If you do find suspicious activity of identity theft or fraud, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. In addition, you should report identity theft to your state's Attorney General and to the Federal Trade Commission ("FTC"). This notice has not been delayed by law enforcement.

Monitoring Your Accounts

You may obtain a free copy of your credit report from each of the credit bureaus once a year by visiting <http://www.annualcreditreport.com>, or calling 877-322-8228. Hearing impaired consumers can access TDD service at 877-730-4104. You may contact the nationwide credit bureaus at:

Equifax, 866-349-5191, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com/FCRA.

Experian, 888-397-3742, P.O. Box 9701, Allen, TX 75013, www.experian.com.

TransUnion, 800-916-8800, P.O. Box 2000, Chester, PA 19022, www.transunion.com.

You may also place a fraud alert or security freeze on your credit report at no cost. A fraud alert is a notice that can be placed on a consumer's credit report that alerts companies who may extend credit that the consumer may have been a victim of identity theft or fraud. When a fraud alert is displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. There are two types of fraud alerts: an "initial" fraud alert that lasts for one year, and an "extended" fraud alert for victims of identity theft or fraud that lasts seven years. A fraud alert should not affect your ability to get a loan or credit, but it may cause some delay if you are applying for credit. To place a fraud alert, please contact one of the credit reporting agencies at:

Equifax, 888-836-6351, P.O. Box 105069, Atlanta, GA 30348, www.equifax.com/personal/credit-report-services.

Experian, 888-397-3742, P.O. Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html.

TransUnion, 800-680-7289, P.O. Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts.

Alternatively, you may place a security freeze on your file. Security freezes will prevent new credit from being opened in your name without the use of a personal identification number or password that will be issued by the credit reporting agencies after you initiate the freeze. In order to place a security freeze, you may be required to provide the credit reporting agencies with information that identifies you. A security freeze can make it more difficult for someone to get credit in your name, but it also may delay your ability to obtain

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

credit. The credit reporting agencies may not charge a fee to place a freeze or remove a freeze. To place a security freeze, please contact one of the agencies at:

Equifax, 888-298-0045, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com/personal/credit-report-services.

Experian, 888-397-3742, P.O. Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html.

TransUnion, 888-909-8872, P.O. Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze.

Additional Information

You may find additional information about fraud alerts, security freezes, and suggestions you can take to protect yourself from identity theft or fraud by contacting the FTC or your state Attorney General.

The FTC provides suggestions for actions you may take in the event of identity theft at www.consumer.ftc.gov/features/feature-0014-identity-theft. You may also call the FTC for more information at 1-877-ID-THEFT (438-4338) (TTY: 1-866-653-4261), or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also review helpful sites to learn more about consumer protection related to information compromise i.e., AHIMA's *Medical Identity Theft Response Checklist for Consumers*, which can be found at <http://bit.ly/2pHDcqV>.

For North Carolina Residents, the North Carolina Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Oregon Residents: the Oregon Attorney General can be contacted at 1162 Court St. NE Salem, OR 97301-4096, 1-877-877-9392, www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/.



Return Mail Processing
PO Box 999
Suwanee, GA 30024

10 1 2325 *****SNGLP

SAMPLE A. SAMPLE - L03

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



August 4, 2023

NOTICE OF DATA BREACH

Dear Parent or Guardian of Sample A. Sample:

We are writing to inform you of a recent incident involving unauthorized access to our computer network. While we have no indication that your minor's personal information has been accessed or misused, some of your minor's information was saved on servers impacted by the incident. We are writing to make you aware of our current understanding of what happened, measures that have been taken, and to provide you with some steps you can take to protect your minor's personal information.

What happened?

On June 13, 2023, we learned that systems on our network were encrypted. We immediately initiated an investigation and retained a leading computer security firm. During the course of the investigation, we learned that there was unauthorized access to systems on the network and that the intruder encrypted files on those systems. We were unable to confirm whether any specific personal information was accessed or acquired. Out of an abundance of caution, we are notifying you of the incident.

What information was involved?

While we were unable to determine whether any of your minor's personal information was accessed or acquired, the following information may have been saved on a server impacted by the incident: first name, last name, date of birth, and social security. To date, we are unaware of any actual or attempted misuse of your minor's personal information as a result of this incident.

What we are doing.

As soon as we learned of this situation, we immediately launched an investigation and retained a leading computer security firm. We took steps to block unauthorized users from connecting to our network and to prevent future security breaches. Based on our current investigation, we believe this incident was limited to this one event.

What you can do.

Although we do not have any evidence that your minor's information has been misused, we recommend that you review the information provided in the enclosed "Further Information and Steps You Can Take." The enclosure identifies some steps you can take to guard against the misuse of your minor's personal information. Never provide personal information in a response to an electronic communication about a data security incident. Additionally, out of an abundance of caution, we are providing identity theft protection services through a one-year membership of Experian's® IdentityWorks Membership at no cost to you. To activate membership and start monitoring your minor's personal information please follow the steps below:

- Ensure that you **enroll by: October 31, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/minorplus>
- Provide your minor's **activation code: ABCDEFGHI**
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks Membership online, please contact Experian's customer care team at 855-797-1033 by **October 31, 2023**, from Monday through Friday 8 am – 10 pm CST, or Saturday and Sunday 10 am – 7 pm CST (excluding major U.S. holidays). Be prepared to provide B100197 as proof of eligibility for the identity restoration services by Experian.

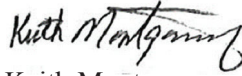
For more information.

We sincerely regret and apologize for any inconvenience this may cause you. Please do not hesitate to contact us at 855-797-1033 if you have any questions or concerns.

Sincerely,



Noriyuki Suzuki, President



Keith Montgomery, Vice President

Enclosure: Further Information and Steps You Can Take

Further Information and Steps You Can Take

Additional details regarding the One-Year Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to \$1M Identity Theft Insurance¹:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 855-797-1033. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze with the three major credit bureaus; and assisting you with contacting government agencies to help restore your minor's identity to its proper condition).

Please note that this Identity Restoration support is available to your minor for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Filing a Police Report for Suspicious Activity

We encourage you to remain vigilant of identity theft or fraud. You should review account statements, explanation of benefits, and credit reports and report any suspicious activity or suspected identity theft. You have the right to file a police report if your minor experiences identity theft or fraud. If you do find suspicious activity of identity theft or fraud, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your minor's records. In addition, you should report identity theft to your state's Attorney General and to the Federal Trade Commission ("FTC"). This notice has not been delayed by law enforcement.

Monitoring Credit Reports

You may obtain a free copy of a credit report from each of the credit bureaus once a year by visiting <http://www.annualcreditreport.com>, or calling 877-322-8228. Hearing impaired consumers can access TDD service at 877-730-4104. You may contact the nationwide credit bureaus at:

Equifax, 866-349-5191, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com/FCRA.

Experian, 888-397-3742, P.O. Box 9701, Allen, TX 75013, www.experian.com.

TransUnion, 800-916-8800, P.O. Box 2000, Chester, PA 19022, www.transunion.com.

A fraud alert or security freeze may be placed on a consumer's credit report at no cost. A fraud alert is a notice that can be placed on a consumer's credit report that alerts companies who may extend credit that the consumer may have been a victim of identity theft or fraud. When a fraud alert is displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. There are two types of fraud alerts: an "initial" fraud alert that lasts for one year, and an "extended" fraud alert for victims of identity theft or fraud that lasts seven years. A fraud alert should not affect a consumer's ability to get a loan or credit, but it may cause some delay when applying for credit. To place a fraud alert, please contact one of the credit reporting agencies at:

Equifax, 888-836-6351, P.O. Box 105069, Atlanta, GA 30348, www.equifax.com/personal/credit-report-services.

Experian, 888-397-3742, P.O. Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html.

TransUnion, 800-680-7289, P.O. Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts.

Alternatively, a consumer may place a security freeze. Security freezes will prevent new credit from being opened in the consumer's name without the use of a personal identification number or password that will be issued by the credit reporting agencies after the freeze

¹ The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

is initiated. In order to place a security freeze, a consumer may be required to provide the credit reporting agencies with information that identifies him or her. A security freeze can make it more difficult for someone to get credit in your name, but it also may delay one's ability to obtain credit. The credit reporting agencies may not charge a fee to place a freeze or remove a freeze. To place a security freeze, please contact one of the agencies at:

Equifax, 888-298-0045, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com/personal/credit-report-services.

Experian, 888-397-3742, P.O. Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html.

TransUnion, 888-909-8872, P.O. Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze.

Additional Information

You may find additional information about fraud alerts, security freezes, and suggestions you can take to guard against identity theft or fraud by contacting the FTC or your state Attorney General.

The FTC provides suggestions for actions you may take in the event of identity theft at www.consumer.ftc.gov/features/feature-0014-identity-theft. You may also call the FTC for more information at 1-877-ID-THEFT (438-4338) (TTY: 1-866-653-4261), or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also review helpful sites to learn more about consumer protection related to information compromise i.e., AHIMA's *Medical Identity Theft Response Checklist for Consumers*, which can be found at <http://bit.ly/2pHDcqV>.

For North Carolina Residents, the North Carolina Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Oregon Residents: the Oregon Attorney General can be contacted at 1162 Court St. NE Salem, OR 97301-4096, 1-877-877-9392, www.doj.state.or.us/consumer-protection/id-theft-data-breaches/data-breaches/.