



September 21, 2022

Ryan M. Cook, Esq.
601.499.8087 (direct)
Ryan.Cook@WilsonElser.com

Via electronic-mail: Idtheft@oag.state.md.us

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

Re:	Our Client	:	iDoxSolutions, Inc.
	Matter	:	Data Security Incident
	Wilson Elser File #	:	16516.01924

Dear Attorney General Frosh:

We represent iDoxSolutions, Inc. (“iDox”) headquartered in Bethesda, Maryland with respect to a data security incident described in more detail below. iDox takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of Maryland residents that were potentially affected, what information has been compromised, and the steps that iDox is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On August 1, 2022, iDox was the target of a ransomware attack that may have resulted in the exposure of personal information. Although we have found no evidence that any information has been specifically accessed for misuse, it is possible that the potentially impacted individuals’ names, address, date of birth and/or social security numbers could have been exposed as a result of this attack.

As of this writing, iDox has not received any reports of related identity theft since the date of the incident (September 21, 2022 to present).

1400 Meadowbrook Road, Suite 100 • Jackson, MS 39211 • p 601.499.8077 • f 601.499.8078

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

wilsonelser.com

2. Maryland Residents Notified

A total of thirty-seven (37) residents of Maryland were potentially affected by this security incident. Notification letters to these individuals were mailed on September 9, 2022, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Immediately upon learning of this incident, iDox contacted a reputable 3rd party forensic team to assist with its investigation. Since then, iDox has been working with law enforcement to help respond to this incident, along with cybersecurity experts to review all policies and procedures relating to the security of iDox's systems.

Although iDox is not aware of any evidence of misuse of personal information, iDox extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through Cyberscout. This service includes 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise. With this protection, Cyberscout will help the affected individuals resolve issues if their identity is compromised.

4. Contact Information

iDox remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Ryan.Cook@WilsonElser.com or 601.499.8087.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Ryan M. Cook, Esq.

Enclosure: *Sample Notification Letters*

iDoxSolutions, Inc
7910 Woodmont Ave Ste 460
Bethesda, MD 20814



Via First-Class Mail

[REDACTED]

September 12, 2022

Notice of Data Incident

[REDACTED]

I am writing to inform you of a network security incident that we (iDox) have experienced. On Monday, August 1, we detected unauthorized activity within our network environment. After discovering the unauthorized activity, our IT professionals, together with third party forensic and cyber-security experts, immediately secured our systems and started recovery operations within a safe and remediated network environment.

We have communicated with our contracting officials to let them know of the incident. While we do not and have never retained any government classified or sensitive data, our clients may have questions. If an individual client reaches out to you with any questions in relation to this incident, please contact me at (301) 646-5257 or via email, so I can provide an appropriate response. The need for accurate and consistent communications with clients and other external parties cannot be understated.

Some of our employees have experienced some operational disruption caused by this event. We are very sorry for any disruption. The third-party incident response firm is conducting a comprehensive forensic investigation to determine the root cause of this incident, as well as whether any sensitive data was compromised during the incident. We look forward to receiving the findings of the forensic investigation as it progresses, and then updating you accordingly.

This security incident may have resulted in unauthorized access to your personal information. At this time, we are unaware of any fraudulent misuse of your personal information. However, we take the privacy of your personal information seriously and want to provide you with information and resources that you can use to protect your information. This letter contains information about the incident and information about how to protect your personal information going forward.

What Happened and What Information was Involved:

As described above, we immediately shut off all access to the network and engaged specialized third-party forensic and technical resources. iDoxSolutions has secured and remediated its network and the data that we maintain.

Once our environment was secure, we immediately initiated a comprehensive investigation into the cause and extent of the unauthorized activity. Although we have found no evidence that your information has been specifically misused as a result of the incident, an investigation revealed that the following categories of employee information may have been exposed to the unauthorized party during the compromise: name, address, date of birth and social security number. We maintain this information for hiring and HR purposes, as you are a current employee of iDoxSolutions. Notably, the types of information affected varied by individual.

As of this writing, iDoxSolutions has not received any reports of related identity theft since the date of the incident.

What We Are Doing:

In light of the incident, we are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for eighteen months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process.

To enroll in Credit Monitoring* services at no charge, please log on to <https://secure.identityforce.com/benefit/idox> and follow the instructions provided. When prompted please provide the following unique code to receive services: WYD9X8THLZ In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

In addition to enrolling with Cyberscout, we encourage you to remain vigilant against incidents of identity theft and fraud by enrolling in this free identify theft protection and credit monitoring. Contact Cyberscout with any questions. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

What You Can Do:

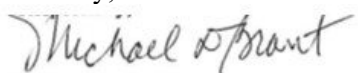
We encourage you to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps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

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

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take.

iDoxSolutions values the privacy and importance of your personal data, and we apologize for any inconvenience or concern that this incident has caused. If you have questions or want additional information, please give me a call at 301-646-5257.

Sincerely,



Mike Brant, CEO
iDoxSolutions, Inc.
(Enclosure)

Steps You Can Take to Help Protect Your Information

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

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

www.experian.com/fraud/center.htmlwww.transunion.com/fraud<https://www.equifax.com/personal/credit-alerts>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

www.experian.com/freeze/center.htmlwww.transunion.com/credit-freeze<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

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

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

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

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

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

iDoxSolutions, Inc
7910 Woodmont Ave Ste 460
Bethesda, MD 20814



Via First-Class Mail

[REDACTED]
[REDACTED]
[REDACTED]

September 12, 2022

Notice of Data Incident

[REDACTED]

I am writing to inform you of a network security incident that we (iDox) have experienced. On Monday, August 1, we detected unauthorized activity within our network environment. After discovering the unauthorized activity, our IT professionals, together with third party forensic and cyber-security experts, immediately secured our systems and started recovery operations within a safe and remediated network environment.

This security incident may have resulted in unauthorized access to your personal information. At this time, we are unaware of any fraudulent misuse of your personal information. However, we take the privacy of your personal information seriously and want to provide you with information and resources that you can use to protect your information. This letter contains information about the incident and information about how to protect your personal information going forward.

What Happened and What Information was Involved:

As described above, we immediately shut off all access to the network and engaged specialized third-party forensic and technical resources. iDoxSolutions has secured and remediated its network and the data that we maintain.

Once our environment was secure, we immediately initiated a comprehensive investigation into the cause and extent of the unauthorized activity. Although we have found no evidence that your information has been specifically misused as a result of the incident, an investigation revealed that the following categories of employee information may have been exposed to the unauthorized party during the compromise: name, address, date of birth and social security number. We maintain this information for hiring and HR purposes, as you are a former employee of iDoxSolutions. Notably, the types of information affected varied by individual.

As of this writing, iDoxSolutions has not received any reports of related identity theft since the date of the incident.

What We Are Doing:

In light of the incident, we are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for eighteen months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process.

To enroll in Credit Monitoring* services at no charge, please log on to <https://secure.identityforce.com/benefit/idox> and follow the instructions provided. When prompted please provide the following unique code to receive services: 3YS2WFJPWB In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

In addition to enrolling with Cyberscout, we encourage you to remain vigilant against incidents of identity theft and fraud by enrolling in this free identify theft protection and credit monitoring. Contact Cyberscout with any questions. Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

What You Can Do:

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

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

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take.

iDoxSolutions values the privacy and importance of your personal data, and we apologize for any inconvenience or concern that this incident has caused. If you have questions or want additional information, please give me a call at 301-646-5257.

Sincerely,



Mike Brant, CEO
iDoxSolutions, Inc.
(Enclosure)

Steps You Can Take to Help Protect Your Information

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

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285

www.experian.com/fraud/center.htmlwww.transunion.com/fraud<https://www.equifax.com/personal/credit-alerts>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045

www.experian.com/freeze/center.htmlwww.transunion.com/credit-freeze<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

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

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

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

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

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