Beckage
Legally Focused. Technology Driven.

Liberty Building, 420 Main Street, Suite 1110, Buffalo, New York 14202
3 Columbus Circle, #1500, New York, New York 10019
600 Broadway, Suite 700, San Diego, California 92101
2 Bala Plaza, Suite 300 #704, Bala Cynwyd, Pennsylvania 19004
75 S. Clinton Ave, 510 Clinton Square, Suite 555, Rochester, New York 14604

July 1, 2021

VIA EMAIL

Office of the Idaho Attorney General
Consumer Protection Division
700 W. Jefferson Street
Boise, ID 83720-0010
agwasden@ag.idaho.gov

Dear Sir or Madam:

On the behalf of our client, Professional Business Systems, Inc. d/b/a Practice*first* Medical Management Solutions and PBS Medcode Corp., ("Practice*first*"), we provide this letter to inform your office of a recent data incident. By providing this notice, Practice*first* does not waive any rights or defenses regarding the applicability of Idaho law, and the applicability of the Idaho data notification laws or personal jurisdiction.

On December 30, 2020, Practice*first* became aware that an unauthorized actor attempted to deploy ransomware to encrypt Practice*first* systems and copied files that contained limited patient and employee personal information (the "Incident"). Upon becoming aware of the Incident, Practice*first* immediately alerted law enforcement, implemented measures to further improve the security of its systems and practices, and worked with a leading privacy and security firm to aide in its investigation and response. After conducting an extensive investigation, Practice*first* was able to determine the extent of the data affected by the Incident, the number of affected individuals, as well as the identity of individuals on May 5, 2021, before concluding the process of confirming state residency on June 25, 2021.

The files copied in this Incident contained the following data elements: name, address, email address, date of birth, driver's license number, Social Security number, diagnosis, laboratory and treatment information, patient identification number, medication information, health insurance identification and claims information, tax identification number, employee username with password, employee username with security questions and answers, and bank account and/or credit card/debit card information. This describes general categories of information involved in this Incident, many records did not include all categories.

A total of 1,210,688 individuals, including 42 Idaho residents, may have been affected by this Incident. Beginning on June 30, 2021, letters were mailed to potentially affected individuals for whom Practice*first* had complete addresses. A copy of the letter mailed to potentially affected individuals is attached hereto. For potentially affected individuals without a complete address, Practice*first* will notify national and state-wide media via press release on July 2, 2021, and posted a notice on its website on June 30, 2021. Practice*first* notified Equifax, TransUnion, and Experian of this Incident on July 1, 2021. Practice*first* is providing two years of Credit Monitoring, Fraud

Consultation, Minor Identity Monitoring, and Identity Theft Restoration services to affected individuals.

Please feel free to contact me with any questions at 716-898-2102 or dgreene@beckage.com.

Sincerely,

Daniel P. Greene, Esq.
Certified Information Privacy Professional, United States (CIPP/US)
Certified Information Privacy Professional, Europe (CIPP/E)

Encls.

June 30, 2021

[redacted]

Dear [redacted],

Professional Business Systems d/b/a Practice*first* Medical Management Solutions and PBS Medcode Corp., ("Practice*first*" or "We") is a medical management company that processes data for health care providers. We write to advise you that We were recently the victim of a data security incident (the "Incident"). We are writing to let you know that this Incident may have affected your personal information ("Information") and, as a precaution, to provide steps you can take to help protect your Information. We are unaware of any misuse of the Information, but We are contacting you to share what We know about the Incident.

What Happened?

On December 30, 2020, We learned that an unauthorized actor who attempted to deploy ransomware to encrypt our systems copied some files from our system, including files that contain limited patient and employee personal Information. Upon learning of this, We shut down our systems, changed passwords, alerted law enforcement, and retained national privacy and security experts.

Our investigation revealed that the Incident involved your Information. We are not aware of any fraud or misuse of any of your Information as a result of this Incident. The actor who took the copy has advised that the Information is destroyed and was not shared.

Why Does Practice*first* Have My Personal Information?

We provide billing and coding services on behalf of health care providers, including hospitals, laboratories, and doctors' offices. We may have your Information because of the services We provide to your health care provider or your employer.

What Information Was Involved?

The Information, copied from our system by the unauthorized actor before it was permanently deleted, included your name and may have included one or more of the following categories of information: address, email address, date of birth, driver's license number, Social Security number, diagnosis, laboratory and treatment information, patient identification number, medication information, health insurance identification and claims information, tax identification number, employee username with password, employee username with security questions and answers, bank account and/or credit card/debit card information. Note that this describes general categories of information involved in this Incident, and likely includes categories that are not relevant to you.

As noted above, We have no evidence that any of your Information was misused.

What We Are Doing.

We immediately reported the Incident to appropriate law enforcement authorities and implemented measures to further improve the security of our systems and practices. We worked with a leading privacy and security firm to aid in our investigation and response, and will report this Incident to relevant government agencies. We also implemented additional security protocols designed to protect our network, email environment, and systems.

What You Can Do.

It is always recommended that you regularly review account statements and report any suspicious activity to financial institutions. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your Information.

While We are unaware of any actual or attempted misuse of your Information as a result of this Incident, We are offering, at no cost to you, two years of identity monitoring services as provided by Kroll, a global leader in risk mitigation and response; their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until **10/28/2021** to activate your identity monitoring services.

Membership Number: [redacted]

Additional information describing your services is included with this letter.

For More Information.

If you have any questions about the Incident or your health care provider(s) that were associated with this Incident, please call 1-855-731-3351, Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding some U.S. national holidays).

Sincerely,

Tom Maher
President & CEO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

June 30, 2021

[redacted]

To the Family of [redacted],

Professional Business Systems d/b/a Practice*first* Medical Management Solutions and PBS Medcode Corp., ("Practice*first*" or "We") is a medical management company that processes data for health care providers. We write to advise you that We were recently the victim of a data security incident (the "Incident"). We are writing to let you know that this Incident may have affected some of your family member's personal information ("Information") and, as a precaution, to provide steps you can take to help protect your family member's Information. We are unaware of any misuse of the Information, but We are contacting you to share what We know about the Incident.

What Happened?

On December 30, 2020, We learned that an unauthorized actor who attempted to deploy ransomware to encrypt our systems copied some files from our system, including files that contain limited patient and employee personal Information. Upon learning of this, We shut down our systems, changed passwords, alerted law enforcement, and retained national privacy and security experts.

Our investigation revealed that the Incident involved your family member's Information. We are not aware of any fraud or misuse of any of your family member's Information as a result of this Incident. The actor who took the copy has advised that the Information is destroyed and was not shared.

Why Does Practice*first* Have My Personal Information?

We provide billing and coding services on behalf of health care providers, including hospitals, laboratories, and doctors' offices. We may have your family member's Information because of the services We provide to your family member's health care provider or your employer.

What Information Was Involved?

The Information, copied from our system by the unauthorized actor before it was permanently deleted, included your family member's name and may have included one or more of the following categories of information: address, email address, date of birth, driver's license number, Social Security number, diagnosis, laboratory and treatment information, patient identification number, medication information, health insurance identification and claims information, tax identification number, employee username with password, employee username with security questions and answers, bank account and/or credit card/debit card information. Note that this describes general categories of information involved in this Incident, and likely includes categories that are not relevant to your family member.

As noted above, We have no evidence that any of your family member's Information was misused.

What We Are Doing.

We immediately reported the Incident to appropriate law enforcement authorities and implemented measures to further improve the security of our systems and practices. We worked with a leading privacy and security firm to aid in our investigation and response, and will report this Incident to relevant government agencies. We also implemented additional security protocols designed to protect our network, email environment, and systems.

What You Can Do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your family member's identity, 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 family member's credit file.

For More Information.

If you have any questions about the Incident or your family member's health care provider(s) that were associated with this Incident, please call 1-855-731-3351, Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding some U.S. national holidays).

Sincerely,

Tom Maher
President & CEO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.

June 30, 2021

[redacted]

Dear Parent or Guardian of [redacted],

Professional Business Systems d/b/a Practice*first* Medical Management Solutions and PBS Medcode Corp., ("Practice*first*" or "We") is a medical management company that processes data for health care providers. We write to advise you that We were recently the victim of a data security incident (the "Incident"). We are writing to let you know that this Incident may have affected some of your child's personal information ("Information") and, as a precaution, to provide steps you can take to help protect your child's Information. We are unaware of any misuse of the Information, but We are contacting you to share what We know about the Incident.

What Happened?

On December 30, 2020, We learned that an unauthorized actor who attempted to deploy ransomware to encrypt our systems copied some files from our system, including files that contain limited patient and employee personal Information. Upon learning of this, We shut down our systems, changed passwords, alerted law enforcement, and retained national privacy and security experts.

Our investigation revealed that the Incident involved your child's Information. We are not aware of any fraud or misuse of any of your child's Information as a result of this Incident. The actor who took the copy has advised that the Information is destroyed and was not shared.

Why Does Practice*first* Have My Personal Information?

We provide billing and coding services on behalf of health care providers, including hospitals, laboratories, and doctors' offices. We may have your child's Information because of the services We provide to your child's health care provider.

What Information Was Involved?

The Information, copied from our system by the unauthorized actor before it was permanently deleted, included your child's name and may have included one or more of the following categories of information: address, email address, date of birth, driver's license number, Social Security number, diagnosis, laboratory and treatment information, patient identification number, medication information, health insurance identification and claims information, and related bank account and/or credit card/debit card information. Note that this describes general categories of information involved in this Incident, and likely includes categories that are not relevant to your child.

As noted above, We have no evidence that any of your child's Information was misused.

What We Are Doing.

We immediately reported the Incident to appropriate law enforcement authorities and implemented measures to further improve the security of our systems and practices. We worked with a leading privacy and security firm to aid in our investigation and response, and will report this Incident to relevant government agencies. We also implemented additional security protocols designed to protect our network, email environment, and systems.

What You Can Do.

It is always recommended that you regularly review account statements for your child and report any suspicious activity to financial institutions. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your child's Information.

While We are unaware of any actual or attempted misuse of your Information as a result of this Incident, We are offering, at no cost to you, two years of identity monitoring services as provided by Kroll, a global leader in risk mitigation and response; their team has extensive experience helping people who have sustained an unintentional exposure of confidential data.

These identity monitoring services include Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration. Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your Minor Identity Monitoring services.

You have until **10/28/2021** to activate your Minor Identity Monitoring services.

Membership Number: [redacted]

Additional information describing your services is included with this letter.

For More Information.

If you have any questions about the Incident or your child's health care provider(s) that were associated with this Incident, please call 1-855-731-3351, Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding some U.S. national holidays).

Sincerely,

Tom Maher
President & CEO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

July 9, 2021

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

Via First Class Mail:

Attorney General Lawrence G. Wasden
Office of the Attorney General
700 W. Jefferson Street
P.O. Box 83720
Boise, ID 83720-0010

Re: Data Incident
Client: Birtcher Anderson and Davis
Our File No. 15991.1007

Dear Attorney General Wasden,

We represent Birtcher Anderson and Davis (hereafter "BAD"), a real estate property and investment management company headquartered in California. This notice is in regard to a cybersecurity incident (hereafter, the "Incident") that occurred at BAD. BAD takes the security and privacy of the information in its control seriously, and took steps to mitigate the effects of the incident occurred.

1. **Nature of the Incident**

On or about May 8, 2021, a BAD employee noticed unusual activity within their files and reached out to the BAD IT Department. BAD's IT team immediately performed an initial investigation and quickly discovered they were undergoing a cybersecurity incident by an unknown threat actor.

Shortly thereafter, BAD engaged a specialized cybersecurity firm to conduct an investigation to determine the nature and scope of the Incident. This investigation concluded on or about May 27, 2021. BAD then performed an examination on their own affected systems and compiled a list of affected individuals. We received this notice list on June 16, 2021. Based on this list, BAD procured credit monitoring for affected individuals, and drafted notices to individuals, consumer credit reporting agencies, and state regulators as appropriate. After further investigation as to the validity of the addresses of the affected individuals, we discovered on July 8, 2021 that 3 of the affected individuals now reside in Idaho.

2. **Number of Idaho residents affected**

3 Idaho residents were potentially affected by the incident. An incident notification letter addressed to the Idaho residents will be mailed pursuant to state law before and no later than July 15, 2021. A sample copy of the notification letter being mailed to potentially affected residents of Idaho is included with this letter.

3. **Steps taken in Response to the Incident**

BAD takes the security and privacy of clients' information very seriously, and has taken steps to protect the privacy of the potentially impacted individuals' information. Specifically, BAD informed our law firm, Wilson Elser Moskowitz Edelman & Dicker LLP, which promptly assisted BAD with responding to the incident. Moreover, upon discovery of this incident, BAD has greatly enhanced its security, including changing passwords. Additionally, we have also obtained complimentary credit monitoring for all affected individuals.

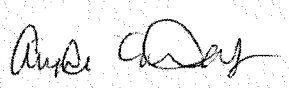
As outlined in the sample notification to the impacted individual, BAD will provide the impacted individuals with complimentary services to help protect their identity. Specifically, BAD has arranged for the impacted individuals to enrol in credit monitoring and identity theft services (including identity theft protection) provided by a third party vendor at no cost to them for 12 months.

4. **Contact Information**

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

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das