

Kevin M. Scott
Tel 312.456.1040
Fax 312.456.8435
scottkev@gtlaw.com

November 13, 2020

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

VIA EMAIL

Dear Attorney General MacDonald:

We are writing to inform you that our client, 1919 Investment Counsel, LLC (“1919ic”), an investment advisory firm headquartered in Baltimore, MD, is notifying 58 individuals who reside in New Hampshire of a data security incident that may have impacted some of their personal information.

On September 21, 2020, a 1919ic employee discovered some unusual activity on their work computer. 1919ic immediately began investigating the potential issue. The investigation included hiring an outside expert forensics firm to analyze the 1919ic systems and determine if there was a breach of security. The investigation revealed that an unauthorized user gained access to 1919ic’s computer systems, which are operated by a third-party managed IT services firm with oversight by 1919ic’s internal technology team. During the forensic analysis, 1919ic was able to quickly take steps to prevent further unauthorized access and secure 1919ic’s systems.

Although we have no evidence that any personal information was accessed or acquired, we notified individuals out of an abundance of caution. The information potentially affected includes customer, employee and/or beneficiary names, addresses, Social Security numbers, 1919ic and custodian account information, photo IDs, dates of birth, bank account information, salary information, benefit information, and contact information obtained and held by 1919ic. This includes clients from Miller Value Partners and Patient Capital Management, on whose behalf 1919ic acts as a service provider, who were separately notified.

Greenberg Traurig, LLP | Attorneys at Law

77 West Wacker Drive | Suite 3100 | Chicago, Illinois 60601 | T +1 312.456.8400 | F +1 312.456.8435

Albany. Amsterdam. Atlanta. Austin. Berlin. Boston. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Las Vegas. London. Los Angeles. Mexico City. Miami. Milan. Minneapolis. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Sacramento. Salt Lake City. San Francisco. Seoul. Shanghai. Silicon Valley. Tallahassee. Tampa. Tel Aviv. Tokyo. Warsaw. Washington, D.C. West Palm Beach. Westchester County.

*Operates as: ~Greenberg Traurig Germany, LLP; *A separate UK registered legal entity; +Greenberg Traurig, S.C.; »Greenberg Traurig Santa Maria; ∞Greenberg Traurig LLP Foreign Legal Consultant Office; ^A branch of Greenberg Traurig, P.A., Florida, USA; ☒GT Tokyo*
Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubegoshi Jimusho; ~Greenberg Traurig Grzesiak sp.k.ACTIVE 53215731v2
www.gtlaw.com

November 13, 2020

Page 2

1919ic is in the process of mailing notifications to all potentially affected individuals in your state between October 16 – November 20, 2020. An example of the notification is attached. 1919ic is offering each potentially affected individual 24 months of 3-bureau credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. 1919ic is also offering parents of minor children who may have been impacted a 24-month subscription to Equifax's Child Identity Monitoring program. Information regarding these services, as well as additional information to assist individuals, is included in the notification.

If you would like additional information concerning the above, please feel free to contact me.

Best regards,



Kevin M. Scott
Shareholder

KMS:

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>> <<Date>>

Re: NOTICE OF DATA BREACH

Dear <<Name 1>>:

1919ic recently was the victim of a security incident that may have impacted some of our current and former employees' personal information. We take the responsibility of protecting our employees' personal information extremely seriously, and we sincerely apologize for any concern this incident may cause.

What Happened?

On September 21, 2020, a 1919ic employee discovered some unusual activity on their 1919ic work computer. We immediately began investigating and retained a third party forensic expert to assist. During our investigation, we learned that an unauthorized user gained access to 1919ic's computer systems, which are operated by a third-party Managed IT services firm with oversight by 1919ic's internal technology team. During the forensic analysis, 1919ic was able to quickly take steps to prevent further unauthorized access and secure our systems. At this time, we do not have any indication that your information was accessed or misused. However, because we deeply value you and are committed to transparency, we wanted to make you aware of this incident.

What information was involved?

The information we hold about our current and former employees may include one or more of the following: name, address, Social Security number, photo ID, birthdate, bank account information, payroll information, and contact information. While we have no evidence that any of this information was viewed by the unauthorized user, we are notifying you because we cannot conclusively rule out that possibility.

What We Are Doing.

We take the security of your information very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence by doing additional monitoring of our networks, further improving access controls, and hardening our systems. As a safeguard, we have also arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*myTrueIdentity*) for two years. This service is provided by TransUnion Interactive, a subsidiary of TransUnion[®], one of the three nationwide credit reporting companies. We have also secured, regardless of enrollment, identity restoration services, including \$1M in identity theft insurance, for two years.

How to Enroll: You can sign up online or via U.S. Mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

What You Can Do

In addition, please review the enclosed “Additional Important Information” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC), regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file, should you choose to do so. You can also contact the FTC for more information.

For More Information

If you have questions regarding enrollment in the credit monitoring service, please call 888-905-0548, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please have your activation code ready.

If you have additional questions or concerns regarding this incident, please feel free to email 1919Assistance@1919ic.com.

Protecting your information is a top priority for us. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "H. O'Mealia". The signature is written in a cursive style with a large initial "H" and a distinct "O'Mealia" portion.

Harry O'Mealia
Chief Executive Officer, President

Additional Important Information

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

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

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of Illinois, Maryland, New York, North Carolina, and Rhode Island:

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

Maryland Office of the Attorney General	Rhode Island Office of the Attorney General	North Carolina Office of the Attorney General	New York Attorney General	Federal Trade Commission
Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	Consumer Protection 150 South Main Street Providence, RI 02903 1-401-274-4400 www.riag.ri.gov	Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.gov	Consumer Frauds & Protection Bureau 120 Broadway - 3rd Floor New York, NY 10271 www.ag.ny.gov	Consumer Response Center 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.identitytheft.gov

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. 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 and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or Transunion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are below.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also 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 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 for yourself or your spouse or a minor under 16: (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; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com
888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19014-0200
www.transunion.com
800-680-7289

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,[®] Experian,[®] and Equifax,[®] including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: NOTICE OF DATA BREACH

Dear <<Salutation>>:

We are writing to inform you of a security incident that may have impacted some of your personal information. 1919 Investment Counsel takes the responsibility of protecting your and all our valued clients' information extremely seriously. We sincerely apologize for any concern this incident may cause.

What Happened?

On September 21, 2020, a 1919ic employee discovered some unusual activity on their 1919ic work computer. We immediately began investigating and retained a third party forensic expert to assist. During our investigation, we learned that an unauthorized user gained access to 1919ic's computer systems, which are operated by a third-party Managed IT services firm with oversight by 1919ic's internal technology team. During the forensic analysis, 1919ic was able to quickly take steps to prevent further unauthorized access and secure our systems. At this time, we do not have any indication that your information was accessed or misused. However, because we deeply value our relationship with you and are committed to transparency, we wanted to make you aware of this incident.

What Information Was Involved?

The information we hold about you may include one or more of the following: name, address, Social Security number, 1919ic and custodian account information, photo ID, birthdate, bank account information, and contact information. While we have no evidence that any of this information was viewed by the unauthorized user, we are notifying you because we cannot conclusively rule out that possibility. **Importantly, the financial custodian responsible for holding your assets was not targeted by the unauthorized user and was not impacted by this incident.** In addition, the 1919ic client access portal was not impacted.

What We Are Doing

We take the security of all information in our systems very seriously, and we want to assure you that we have already taken steps to prevent a recurrence by doing additional monitoring of our networks, further improving access controls, and hardening our systems. As a safeguard, we have also arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*myTrueIdentity*) for two years. This service is provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. We have also secured, regardless of enrollment, identity restoration services, including \$1M in identity theft insurance, for two years.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at **www.MyTrueIdentity.com** and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<**Insert Unique 12-letter Activation Code**>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<**Insert static 6-digit Telephone Pass Code**>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<**Enrollment Deadline**>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

What You Can Do

In addition, please review the enclosed “Additional Important Information” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file, should you choose to do so. You can also contact the FTC for more information.

For More Information

If you have questions regarding enrollment in the credit monitoring service, please call 888-905-0548, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please have your activation code ready.

If you have additional questions or concerns regarding this incident, please feel free to contact a member of your portfolio team or send an email to 1919Assistance@1919ic.com.

Protecting your information is a top priority for us. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,



Harry O'Mealia
Chief Executive Officer, President

Additional Important Information

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

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

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of Illinois, Maryland, New York, North Carolina, and Rhode Island:

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

Maryland Office of the Attorney General	Rhode Island Office of the Attorney General	North Carolina Office of the Attorney General	New York Attorney General	Federal Trade Commission
Consumer Protection Division	Consumer Protection	Consumer Protection Division	Consumer Frauds & Protection Bureau	Consumer Response Center
200 St. Paul Place	150 South Main Street	9001 Mail Service Center	120 Broadway - 3rd Floor	600 Pennsylvania Ave, NW
Baltimore, MD 21202	Providence, RI 02903	Raleigh, NC 27699-9001	New York, NY 10271	Washington, DC 20580
1-888-743-0023	1-401-274-4400	1-877-566-7226	www.ag.ny.gov	1-877-IDTHEFT (438-4338)
www.oag.state.md.us	www.riag.ri.gov	www.ncdoj.gov		www.identitytheft.gov

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. 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 and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (<https://www.experian.com/fraud/center.html>), or TransUnion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also 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 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 for yourself or your spouse or a minor under 16: (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; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com
888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19014-0200
www.transunion.com
800-680-7289

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian®, and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)



MILLER
VALUE
PARTNERS

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: NOTICE OF DATA BREACH

Dear <<Name 1>>:

We are writing to inform you of a security incident that may have impacted some of your personal information. Miller Value Partners, LLC takes the responsibility of protecting your and all our valued clients' information extremely seriously. We sincerely apologize for any concern this incident may cause.

What Happened?

On September 21, 2020, an employee of our technology service provider discovered some unusual activity on our network. Our service provider immediately began investigating and retained a third party forensic expert to assist. As a result of the investigation, we learned that an unauthorized user gained access to our computer systems, which are operated by a third-party Managed IT services firm. During the forensic analysis, our service provider was able to quickly take steps to prevent further unauthorized access and secure our systems. At this time, we do not have any indication that your information was accessed or misused. However, because we deeply value our relationship with you and are committed to transparency, we wanted to make you aware of this incident.

What information was involved?

The information we hold about you may include one or more of the following: name, address, Social Security number, custodian account information, photo ID, birthdate, bank account information, and contact information. While we have no evidence that any of this information was viewed by the unauthorized user, we are notifying you because we cannot conclusively rule out that possibility. **Importantly, the financial custodian responsible for holding your assets was not targeted by the unauthorized user and was not impacted by this incident.**

What We Are Doing

We take the security of all information in our systems very seriously, and we want to assure you that we have already taken steps to prevent a recurrence by doing additional monitoring of our networks, further improving access controls, and hardening our systems. As a safeguard, we have also arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*myTrueIdentity*) for two years. This service is provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. We have also secured, regardless of enrollment, identity restoration services, including \$1M in identity theft insurance, for two years.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

What You Can Do

In addition, please review the enclosed “Additional Important Information” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file, should you choose to do so. You can also contact the FTC for more information.

For More Information

If you have questions regarding enrollment in the credit monitoring service, please call 888-905-0548, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please have your activation code ready.

If you have additional questions or concerns regarding this incident, please feel free to contact us at 410-454-3130 or send an email to MVPAssistance@MillerValue.com.

Protecting your information is a top priority for us. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

Neil O’Callaghan
President & Chief Compliance Officer

Additional Important Information

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

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

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of Illinois, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity

Maryland Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street Providence, RI 02903 1-401-274-4400 www.riag.ri.gov	North Carolina Office of the Attorney General Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.gov	New York Attorney General Consumer Frauds & Protection Bureau 120 Broadway - 3rd Floor New York, NY 10271 www.ag.ny.gov	Federal Trade Commission Consumer Response Center 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.identitytheft.gov
---	--	--	---	---

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. 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 and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf)), Experian (<https://www.experian.com/fraud/center.html>), or TransUnion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also 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 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 for yourself or your spouse or a minor under 16: (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; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
www.experian.com
888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19014-0200
www.transunion.com
800-680-7289

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian®, and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: NOTICE OF DATA BREACH

Dear <<Name 1>>:

We are writing to inform you of a security incident that may have impacted some of your personal information. Patient Capital Management, LLC takes the responsibility of protecting your and all our valued clients' information extremely seriously. We sincerely apologize for any concern this incident may cause.

What Happened?

On September 21, 2020, an employee of our technology service provider discovered some unusual activity on our network. Our service provider immediately began investigating and retained a third party forensic expert to assist. As a result of the investigation, we learned that an unauthorized user gained access to our computer systems, which are operated by a third-party Managed IT services firm. During the forensic analysis, our service provider was able to quickly take steps to prevent further unauthorized access and secure our systems. At this time, we do not have any indication that your information was accessed or misused. However, because we deeply value our relationship with you and are committed to transparency, we wanted to make you aware of this incident.

What information was involved?

The information we hold about you may include one or more of the following: name, address, Social Security number, custodian account information, photo ID, birthdate, bank account information, and contact information. While we have no evidence that any of this information was viewed by the unauthorized user, we are notifying you because we cannot conclusively rule out that possibility. **Importantly, the financial custodian responsible for holding your assets was not targeted by the unauthorized user and was not impacted by this incident.**

What We Are Doing

We take the security of all information in our systems very seriously, and we want to assure you that we have already taken steps to prevent a recurrence by doing additional monitoring of our networks, further improving access controls, and hardening our systems. As a safeguard, we have also arranged for you to enroll, at no cost to you, in an online, three-bureau credit monitoring service (*myTrueIdentity*) for two years. This service is provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. We have also secured, regardless of enrollment, identity restoration services, including \$1M in identity theft insurance, for two years. This service is provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies. We have also secured, regardless of enrollment, identity restoration services, including \$1M in identity theft insurance, for two years.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

What You Can Do

In addition, please review the enclosed “Additional Important Information” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file, should you choose to do so. You can also contact the FTC for more information.

For More Information

If you have questions regarding enrollment in the credit monitoring service, please call 888-905-0548, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please have your activation code ready.

If you have additional questions or concerns regarding this incident, please feel free to contact us at 410-454-3130 or send an email to PatientAssistance@PatientCM.com.

Protecting your information is a top priority for us. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

Neil O’Callaghan
Chief Compliance Officer

Additional Important Information

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

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

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of Illinois, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity

Maryland Office of the Attorney General Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street Providence, RI 02903 1-401-274-4400 www.riag.ri.gov	North Carolina Office of the Attorney General Consumer Protection Division 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.gov	New York Attorney General Consumer Frauds & Protection Bureau 120 Broadway - 3rd Floor New York, NY 10271 www.ag.ny.gov	Federal Trade Commission Consumer Response Center 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.identitytheft.gov
---	--	--	---	---

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. 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 and online with Equifax ([https://assets.equifax.com/assets/personal/Fraud Alert Request Form.pdf](https://assets.equifax.com/assets/personal/Fraud%20Alert%20Request%20Form.pdf)), Experian (<https://www.experian.com/fraud/center.html>), or TransUnion (<https://www.transunion.com/fraud-victim-resource/place-fraud-alert>). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also 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 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 for yourself or your spouse or a minor under 16: (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; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
www.experian.com
888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19014-0200
www.transunion.com
800-680-7289

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, Experian®, and Equifax®, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)