

17573

APPENDIX A

P I M C O

September 2, 2020

Dear Investor,

We are writing to notify you of a data security incident involving a third-party vendor used by SEI Investments Company ("SEI"), which provides administrative services to PIMCO and certain PIMCO-advised private funds. The vendor, M. J. Brunner, Inc. ("Brunner"), manages the SEI Investor Dashboard portal ("SEI Portal") and assists SEI with website and application development and maintenance.

The incident impacted Brunner's corporate network and resulted in the unauthorized acquisition and online disclosure of certain PIMCO account statements as well as other data elements related to SEI Portal user profiles that were stored on Brunner's corporate network. Based on our correspondence with SEI, we believe that your December 31, 2016 PIMCO account statements and data elements related to your SEI Portal user profile were impacted in the breach.

**What happened:** SEI has advised us that Brunner first became aware of suspicious activity on its corporate network on May 17, 2020, and notified SEI on that day. At that time, based on information provided by SEI, it is our understanding that SEI was not aware that its client data was at risk. We understand that Brunner received additional information in connection with the attack on or around June 9, 2020. SEI has advised us that on that day SEI learned that the data incident impacting Brunner's corporate network had impacted some of its clients' data. On or about June 29, 2020, SEI informed PIMCO that SEI's third-party vendor was the victim of a cyber attack but was not aware at that stage of the specific details of the incident nor the extent to which any PIMCO information was compromised as a result of the incident. SEI noted that it was continuing its investigation. On July 20, 2020 and July 21, 2020, SEI informed us that certain PIMCO client data was compromised as a result of the data incident experienced by Brunner. SEI said that the impacted data related to users of the SEI Portal, as well as certain account statements that Brunner stored on its corporate networks on SEI's behalf. SEI informed us that the incident had impacted PIMCO clients and investors who used the SEI Portal and whose PIMCO account statements were stored on Brunner corporate networks, and that the breach had resulted in the unauthorized disclosure of that data online.

**What information was involved:** Based on our discussions with SEI and as a result of information SEI learned through its investigation, we believe that the following categories of information about you were compromised and have been disclosed online by unauthorized actors:

- Name
- SEI account identification number
- Email address
- Phone number used to register for the SEI Portal
- Your SEI Portal username
- PIMCO Account Number
- Address
- Beginning/ending account balance
- Quarterly fee in light of the account balance

17573

APPENDIX A

P I M C O

September 2, 2020

Dear Investor,

We are writing to notify you of a data security incident involving a third-party vendor used by SEI investments Company ("SEI"), which provides administrative services to PIMCO and certain PIMCO-advised private funds. The vendor, M. J. Brunner, Inc. ("Brunner"), manages the SEI Investor Dashboard portal ("SEI Portal") and assists SEI with website and application development and maintenance.

The incident impacted Brunner's corporate network and resulted in the unauthorized acquisition and online disclosure of certain PIMCO account statements as well as other data elements related to SEI Portal user profiles that were stored on Brunner's corporate network. Based on our correspondence with SEI, we believe that your December 31, 2016 PIMCO account statements and data elements related to your SEI Portal user profile were impacted in the breach.

**What happened:** SEI has advised us that Brunner first became aware of suspicious activity on its corporate network on May 17, 2020, and notified SEI on that day. At that time, based on information provided by SEI, it is our understanding that SEI was not aware that its client data was at risk. We understand that Brunner received additional information in connection with the attack on or around June 9, 2020. SEI has advised us that on that day SEI learned that the data incident impacting Brunner's corporate network had impacted some of its clients' data. On or about June 29, 2020, SEI informed PIMCO that SEI's third-party vendor was the victim of a cyber attack but was not aware at that stage of the specific details of the incident nor the extent to which any PIMCO information was compromised as a result of the incident. SEI noted that it was continuing its investigation. On July 20, 2020 and July 21, 2020, SEI informed us that certain PIMCO client data was compromised as a result of the data incident experienced by Brunner. SEI said that the impacted data related to users of the SEI Portal, as well as certain account statements that Brunner stored on its corporate networks on SEI's behalf. SEI informed us that the incident had impacted PIMCO clients and investors who used the SEI Portal and whose PIMCO account statements were stored on Brunner corporate networks, and that the breach had resulted in the unauthorized disclosure of that data online.

**What information was involved:** Based on our discussions with SEI and as a result of information SEI learned through its investigation, we believe that the following categories information about you were compromised and have been disclosed online by unauthorized actors:

- Name
- SEI account identification number
- Email address
- Phone number used to register for the SEI Portal
- Your SEI Portal username
- PIMCO Account Number
- Address
- Beginning/ending account balance
- Quarterly fee in light of the account balance

- The fact that you are associated with PIMCO as an investor, client or other interested party.

SEI has also informed us on August 13, 2020 that your SEI Portal password, security questions and answers were exposed, but that those data elements were encrypted. SEI has confirmed to us that it has no reason to believe that the attackers accessed unencrypted versions of those data elements or that any SEI Portal accounts were accessed by unauthorized persons as a result.

**Steps we are taking:** We have remained in regular contact with SEI throughout its investigation of the incident in order to determine what happened and in order to get regular updates regarding the incident and its impact on our clients. It is our understanding that SEI has conducted a review to determine the extent of the data compromised and that it has worked with Brunner and several external cybersecurity experts to investigate and remediate the incident. Applicable law enforcement authorities have been notified of the incident.

In addition, SEI is offering a complimentary one-year membership of Experian's® IdentityWorks<sup>SM</sup>. If you would like to accept this offer, please follow the steps set out in Appendix A.

**Steps you can take:** We recommend that you immediately take the following steps:

- Sign up for the Experian IdentityWorks credit services by following the instructions provided in **Appendix A**.
- Update your password to the SEI Portal if you have not done so already.
- Remain vigilant by reviewing your account statements and credit reports for any unauthorized activity and remain particularly vigilant to potential phishing attempts by email or phone. Other than a one-time pin, neither SEI nor PIMCO will email or call you with links to reset your password.

In addition, we recommend that you please read and consider undertaking the following actions.

**(i) Obtain Your Free Credit Report**

You are entitled to receive your credit report from each of the three national credit reporting agencies every twelve months, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling 1-877-322-8228 or by completing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) and mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

When you receive your credit report(s), please review them carefully. Look for accounts you did not open or do not recognize, or requests for your credit report from anyone that you did not apply for credit with. Look for personal information, such as a home address or Social Security number, that is not accurate. If you see anything you do not understand or that is incorrect, notify the appropriate credit reporting agency as soon as possible.

**(ii) Place a Fraud Alert on Your Credit Files**

To further protect you from the possibility of identity theft, each of the national credit reporting agencies provides the ability to place a fraud alert on your credit card files. A fraud alert notifies any creditors that access your credit report that you may be the victim of fraud and encourages them to take additional steps to protect you from fraud. You may place a fraud alert by calling the toll-free numbers below for each or any of the credit reporting agencies and requesting that a fraud alert be placed on your credit file.

Additional information is available at [www.consumer.ftc.gov/articles/0275-place-fraud-alert](http://www.consumer.ftc.gov/articles/0275-place-fraud-alert).

**Experian**

[www.experian.com](http://www.experian.com)  
1-888-397-3742

**Equifax**

[www.equifax.com](http://www.equifax.com)  
1-888-836-6351

**TransUnion**

[www.transunion.com](http://www.transunion.com)  
1-800-680-7289

**(iii) Review Your Account Statements Regularly**

We recommend that you closely monitor your banking and credit account statements for suspicious activity on your existing accounts. You should remain vigilant by attentively monitoring your credit reports and account statements for indications of fraud and/or theft, including identity theft.

**(iv) Consider Placing a Security Freeze on Your Credit File**

If you have placed a fraud alert, but still believe you are at risk, you should be aware that you may also place a security freeze on your credit file. A security freeze means that your file cannot be shared with potential creditors to open new cards or other lines of credit without your express authorization. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. Requests for security freezes are processed through each of the national reporting agencies noted above. There is no charge to place a security freeze.

In order to request a security freeze, you will need to provide some or all of the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
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;

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals

you would like to receive your credit report or the specific period of time you want the credit report available.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze.

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of requests you make for credit, loans or other services. For more information, contact the credit reporting agencies directly.

You can request a security freeze free of charge by contacting the credit bureaus. If submitting a request by mail, you may need to provide a credit bureau with a completed form and certain verification information.

**Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

**Equifax**

Equifax Information Services LLC  
P.O. Box 105788  
Atlanta, GA 30348-5788  
[www.equifax.com](http://www.equifax.com)  
[1-888-298-0045](tel:1-888-298-0045)

**TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
[www.transunion.com](http://www.transunion.com)  
[1-888-909-8872](tel:1-888-909-8872)

**(v) Review Information From the U.S. Federal Trade Commission**

You may wish to review the tips provided by the Federal Trade Commission ("FTC") on how to avoid identity theft, or learn more from the FTC about how to place a fraud alert or security freeze. For more information, please visit <http://www.ftc.gov/idtheft> or call 1-800-ID-THEFT. The FTC is located at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**More Information**

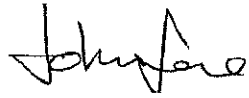
- **For Massachusetts Residents:** Massachusetts residents have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**Questions**

PIMCO is here to help you and if you have any further questions or concerns please contact your PIMCO Account Manager.

Please know that PIMCO, an indirect subsidiary of Allianz SE, takes this matter very seriously and we apologize for any concern and inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "John Lane". The signature is fluid and cursive, with the first name "John" being more prominent than the last name "Lane".

John Lane

Executive Vice President and Global Chief Financial Officer of Alternatives of Pacific Investment  
Management Company LLC

## Appendix A

SEI is offering a complimentary one-year membership of Experian's® IdentityWorks<sup>SM</sup> to any U.S. domiciled person. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: October 31, 2020 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code**: **(Please keep this code confidential)**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by **October 31, 2020**. Be prepared to provide engagement number DB21491 as proof of eligibility for the identity restoration services by Experian.

## APPENDIX B

# PIMCO

September 2, 2020

Dear Investor,

We are writing to notify you of a data security incident involving a third-party vendor used by SEI investments Company ("SEI"), which provides administrative services to PIMCO and certain PIMCO-advised private funds. The vendor, M. J. Brunner, Inc. ("Brunner"), manages the SEI Investor Dashboard portal ("SEI Portal") and assists SEI with website and application development and maintenance.

The incident impacted Brunner's corporate network and resulted in the unauthorized acquisition and online disclosure of certain PIMCO account statements and Bravo II Fund capital call statements, as well as other data elements related to SEI Portal user profiles that were stored on Brunner's corporate network. Based on our correspondence with SEI, we believe that your December 31, 2016 PIMCO account statements, Bravo Fund II capital call notice dated February 28, 2017 and data elements related to your SEI Portal user profile were impacted in the breach.

**What happened:** SEI has advised us that Brunner first became aware of suspicious activity on its corporate network on May 17, 2020, and notified SEI on that day. At that time, based on information provided by SEI, it is our understanding that SEI was not aware that its client data was at risk. We understand that Brunner received additional information in connection with the attack on or around June 9, 2020. SEI has advised us that on that day, SEI learned that the data incident impacting Brunner's corporate network had impacted some of its clients' data. On or about June 29, 2020, SEI informed PIMCO that SEI's third-party vendor was the victim of a cyber attack but was not aware at that stage of the specific details of the incident nor the extent to which any PIMCO information was compromised as a result of the incident. SEI noted that it was continuing its investigation. On July 20, 2020 and July 21, 2020, SEI informed us that certain PIMCO client data was compromised as a result of the data incident experienced by Brunner. SEI said that the impacted data related to users of the SEI Portal, as well as certain account statements and Bravo Fund II capital call statements that Brunner stored on its corporate networks on SEI's behalf. SEI informed us that the incident had impacted PIMCO clients and investors who used the SEI Portal and whose PIMCO account statements and Bravo Fund II capital call statements were stored on Brunner corporate networks, and that the breach had resulted in the unauthorized disclosure of that data online.

**What information was involved:** Based on our discussions with SEI and as a result of information SEI learned through its investigation, we believe that the following categories information about you were compromised and have been disclosed online by unauthorized actors:

- Name
- SEI account identification number
- Email address
- Phone number used to register for the SEI Portal
- Your SEI Portal username
- Information related to the Bravo Fund II capital call, such as the value of your capital commitment and the amount of the capital call
- PIMCO Account Number
- Address



- Beginning/ending account balance
- Quarterly fee in light of the account balance
- The fact that you are associated with PIMCO as an investor, client or other interested party.

SEI has also informed us on August 13, 2020 that your SEI Portal password, security questions and answers were exposed, but that those data elements were encrypted. SEI has confirmed to us that it has no reason to believe that the attackers accessed unencrypted versions of those data elements or that any SEI Portal accounts were accessed by unauthorized persons as a result.

**Steps we are taking:** We have remained in regular contact with SEI throughout its investigation of the incident in order to determine what happened and in order to get regular updates regarding the incident and its impact on our clients. It is our understanding that SEI has conducted a review to determine the extent of the data compromised and that it has worked with Brunner and several external cybersecurity experts to investigate and remediate the incident. Applicable law enforcement authorities have been notified of the incident.

In addition, SEI is offering a complimentary one-year membership of Experian's® IdentityWorks<sup>SM</sup>. If you would like to accept this offer, please follow the steps set out in Appendix A.

**Steps you can take:** We recommend that you immediately take the following steps:

- Sign up for the Experian IdentityWorks credit services by following the instructions provided in **Appendix A**.
- Update your password to the SEI Portal if you have not done so already.
- Remain vigilant by reviewing your account statements and credit reports for any unauthorized activity and remain particularly vigilant to potential phishing attempts by email or phone. Other than a one-time pin, neither SEI nor PIMCO will email or call you with links to reset your password.

In addition, we recommend that you please read and consider undertaking the following actions.

**(i) Obtain Your Free Credit Report**

You are entitled to receive your credit report from each of the three national credit reporting agencies every twelve months, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling 1-877-322-8228 or by completing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) and mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

When you receive your credit report(s), please review them carefully. Look for accounts you did not open or do not recognize, or requests for your credit report from anyone that you did not apply for credit with. Look for personal information, such as a home address or Social Security number, that is not accurate. If you see anything you do not understand or that is incorrect, notify the appropriate credit reporting agency as soon as possible.

**(ii) Place a Fraud Alert on Your Credit Files**

To further protect you from the possibility of identity theft, each of the national credit reporting agencies provides the ability to place a fraud alert on your credit card files. A fraud alert notifies any creditors that access your credit report that you may be the victim of fraud and encourages them to take additional steps to protect you from fraud. You may place a fraud alert by calling the toll-free numbers below for each or any of the credit reporting agencies and requesting that a fraud alert be placed on your credit file.

Additional information is available at [www.consumer.ftc.gov/articles/0275-place-fraud-alert](http://www.consumer.ftc.gov/articles/0275-place-fraud-alert).

**Experian**

[www.experian.com](http://www.experian.com)

1-888-397-3742

**Equifax**

[www.equifax.com](http://www.equifax.com)

1-888-836-6351

**TransUnion**

[www.transunion.com](http://www.transunion.com)

1-800-680-7289

**(iii) Review Your Account Statements Regularly**

We recommend that you closely monitor your banking and credit account statements for suspicious activity on your existing accounts. You should remain vigilant by attentively monitoring your credit reports and account statements for indications of fraud and/or theft, including identity theft.

**(iv) Consider Placing a Security Freeze on Your Credit File**

If you have placed a fraud alert, but still believe you are at risk, you should be aware that you may also place a security freeze on your credit file. A security freeze means that your file cannot be shared with potential creditors to open new cards or other lines of credit without your express authorization. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. Requests for security freezes are processed through each of the national reporting agencies noted above. There is no charge to place a security freeze.

In order to request a security freeze, you will need to provide some or all of the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
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;

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals

you would like to receive your credit report or the specific period of time you want the credit report available.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze.

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of requests you make for credit, loans or other services. For more information, contact the credit reporting agencies directly.

You can request a security freeze free of charge by contacting the credit bureaus. If submitting a request by mail, you may need to provide a credit bureau with a completed form and certain verification information.

**Experian Security Freeze**

P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742

**Equifax**

Equifax Information Services LLC  
P.O. Box 105788  
Atlanta, GA 30348-5788  
[www.equifax.com](http://www.equifax.com)  
[1-888-298-0045](tel:1-888-298-0045)

**TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
[www.transunion.com](http://www.transunion.com)  
[1-888-909-8872](tel:1-888-909-8872)

**(v) Review Information From the U.S. Federal Trade Commission**

You may wish to review the tips provided by the Federal Trade Commission ("FTC") on how to avoid identity theft, or learn more from the FTC about how to place a fraud alert or security freeze. For more information, please visit <http://www.ftc.gov/idtheft> or call 1-800-ID-THEFT. The FTC is located at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**More Information**

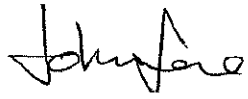
- **For Massachusetts Residents:** Massachusetts residents have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**Questions**

PIMCO is here to help you and if you have any further questions or concerns please contact your PIMCO Account Manager.

Please know that PIMCO, an indirect subsidiary of Allianz SE, takes this matter very seriously and we apologize for any concern and inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "John Lane". The signature is fluid and cursive, with the first name "John" being more prominent than the last name "Lane".

John Lane

Executive Vice President and Global Chief Financial Officer of Alternatives of Pacific Investment  
Management Company LLC

## Appendix A

SEI is offering a complimentary one-year membership of Experian's® IdentityWorks<sup>SM</sup> to any U.S. domiciled person. This product provides you with identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** October 31, 2020 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code:** **(Please keep this code confidential)**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-890-9332 by **October 31, 2020**. Be prepared to provide engagement number DB21491 as proof of eligibility for the identity restoration services by Experian.

