Mark C. Trenchard
Director, Operational Compliance
Legal/Compliance
617-760-3601
617-255-9120 fax
mark_trenchard@putnam.com

7 Shattuck Road
Andover, MA 01810

Putnam INVESTMENTS

July 13, 2018

Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Dear Sir or Madam:

I am writing on behalf of Putnam Investor Services, Inc. (Putnam), transfer agent for the Putnam mutual funds, to notify the New Hampshire Office of the Attorney General of a recent data security incident involving four New Hampshire residents.

On April 20, 2018, we discovered that an employee of a contractor Putnam retained to work on a conversion of our Human Resources Information Management ("HRIM") system attached a document with an embedded file containing the names and Social Security numbers of four current or former Putnam employees to a draft personal e-mail account. Putnam's Data Loss Prevention ("DLP") system, immediately detected the activity and the DLP program administrator contacted the contractor's employee for an explanation of the activity. Unfortunately, the activity occurred on the individual's last day working on the Putnam project, so we have had to work through the contractor to gain an understanding of the activity.

Putnam's Compliance department discussed the incident with the contractor and its employee. The contactor's employee stated that he intended to only append personal files to the draft personal e-mail account for the purpose of recovering them from his Putnam-issued laptop prior to his departure. The individual has stated that he inadvertently attached the Putnam document containing the embedded file to the draft e-mail and that he removed it from the draft immediately after being notified that the document contained nonpublic personally identifiable information for sixteen current or former Putnam employees. The contractor's employer subsequently allowed Putnam to inspect his personal e-mail account, and we confirmed there was no record of the

document with the embedded file in various folders within his account. The contractor's employee has since provided a written attestation stating that he (1) deleted the file from his personal e-mail account, (2) did not transmit the file from his personal e-mail account, and (3) did not misuse the file or the data contained therein for any unauthorized purpose.

To our knowledge, none of the impacted employees, including the New Hampshire residents, have experienced identity theft as a result of the incident. Nevertheless, Putnam has offered free credit monitoring to the affected employees for two years.

Putnam has notified the New Hampshire residents by personal letter, a copy of which is enclosed. The correspondence includes information on preventing identity theft, instructions how to activate free credit monitoring for two years, and a telephone number they may call to obtain further information on the incident.

Please do not hesitate to contact me at 1-617-760-3601 if you have any questions regarding the security incident or Putnam's response.

Sincerely,

Mark Trenchard

Mark C. Trenchard

Enclosure: Shareholder Notification Letter

Putnam INVESTMENTS

One Post Office Square
Boston, MA 02109
www.putnam.com

@@@@DATE@@@

@@REGLINE 1@@
@@REGLINE 2@@
@@REGLINE 3@@
@@REGLINE 4@@
@@REGLINE 5@@

Re: IMPORTANT NOTICE ABOUT YOUR PERSONAL INFORMATION

Dear Shareholder:

We are writing to you because of a recent security incident involving your personal information. We discovered that an employee of a Putnam contractor attached a file to a draft email on his personal e-mail account which included your name and Social Security number.

On April 20, 2018, Putnam's Data Loss Prevention system ('DLP") identified the aforementioned activity. Representatives from Putnam's Legal and Compliance department discussed this incident with the contractor and its employee, who stated that he intended only to recover his own personal files before completing his assignment at Putnam by appending them to his personal e-mail account; however, while attaching his personal files he included a Putnam file that contained your personal information. The contractor's employee has stated that he deleted the draft email on the same day he was notified that of the unauthorized activity by the administrator of Putnam's DLP. The contractor's employee allowed Putnam to access his personal e-mail account and we confirmed that the file had not been retained in various folders within his personal e-mail account.

Please be assured that we have taken every step necessary to address the incident, and that we are committed to protecting all the information that has been entrusted to us. Out of an abundance of caution, we are offering a complimentary two-year membership of Experian's® IdentityWorks SM. This product provides you with superior identity detection and resolution of identity theft. For more information on identity theft prevention and IdentityWorks SM, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.

We have absolutely no evidence of unauthorized use of your personal data and we have no reason to believe any such use is likely; however, we wanted to inform you of the incident and steps you may wish to take to protect yourself. We will assist you to protect yourself in the highly unlikely event that the above-described incident gives rise to unauthorized use of your personal information. You may wish to monitor the activity on your credit report, and tools are available to help you do so. You may wish to be vigilant for the next 12 months, for example, by carefully reviewing your credit reports and bank, credit card and other account statements. If you discover suspicious activity on your credit report, your accounts or by any other means, please call your local police and file a report of identity theft. Also, please notify us of any suspicious activity. A list of protective steps you may take is included with this letter.

Hopefully this letter provides you with the information you need, but please do not hesitate to call at 1-800-225-1581, if we can assist you further.

Sincerely,

John R. Cashman
Operational Compliance
Putnam Investments

To help protect your identity, we are offering a **complimentary two years** membership of Experian's® IdentityWorks SM. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **October 31, 2018** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your **activation code**: **TFKTTP7D3**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **October 31, 2018.** Be prepared to provide engagement number **DB07718** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR TWO-YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

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

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

Proactive Steps You May Take to Protect Your Information

- Remain vigilant for the next 12 to 24 months.

Carefully review your credit reports and bank, credit card and other account statements. We also encourage you to report suspected identity theft to the Federal Trade Commission, law enforcement or your attorney general's office.

- Place a 90-day fraud alert on your credit file.

A fraud alert notifies creditors that you may be the victim of fraud and tells them to contact you before opening any new accounts. Please call any one of the three nationwide consumer reporting agencies listed below. By calling one reporting agency, the other two will automatically be notified. They will place a fraud alert on your credit file and will assist you in getting a free credit report from each of the three agencies. The initial fraud alert will last for 90 days. You may want to renew it after the first 90 days. If you have already filed an identity theft report with your local police department, you should place an extended fraud alert on your credit file. This fraud alert is a free service and is valid for 7 years.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9532	Fraud Victim Assistance
Atlanta, GA 30374-0241	Allen, TX 75013	Division
1-800-525-6285	1-888-397-3742	P.O. Box 6790
www.equifax.com	www.experian.com	Fullerton, CA 92834-6790
		1-800-680-7289
		www.transunion.com

- Place a security freeze on your credit report.

Residents of some states are permitted to place a freeze on their credit report. The security freeze will prohibit a consumer reporting agency from releasing any information in your consumer report without your express authorization. The security freeze is designed to prevent credit, loans or services from being approved in your name without your consent. You should be aware that using a security freeze may delay, interfere with, or prevent the timely approval of any subsequent credit request or application you make regarding new loans. To initiate a credit freeze or to place a fraud alert on your credit report contact one of the three credit reporting agencies listed above.

- Order your free annual credit reports.

To order your free annual credit reports, call toll-free 1-877-322-8228, visit www.annualcreditreport.com, or complete the Annual Credit Report Request Form online and mail to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Hearing impaired consumers can access the TDD service at 1-877-730-4104. For your free annual credit report, do not contact the three nationwide consumer

reporting companies individually; they provide this service only through www.annualcreditreport.com.

- When you receive your credit reports, review them carefully.

Once you receive your credit reports, review them carefully. Please look for accounts you did not open or inquiries from creditors that you did not initiate. Verify all the information is accurate. If you have questions or notice inaccurate information, please call the consumer reporting agency at the telephone number listed on the report.

- Learn more about identity theft and ways to protect yourself.

The Federal Trade Commission has on-line guidance about the steps that consumers can take to protect themselves against identity theft. You can call 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261; write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or visit the Federal Trade Commission's website at www.ftc.gov/idtheft to get more information.

Maryland residents may also obtain additional information on avoiding identity theft from the Office of the Attorney General at the address below, by telephone, or on their website (http://www.oag.state.md.us/index.htm).

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202