March 18, 2024

VIA E-Mail - consumer@ag.iowa.gov

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

RE: Update to Notice of Security Event

To Whom it May Concern:

We (Fidelity Investments Life Insurance Company & Empire Fidelity Life Insurance Company) are writing to supplement our initial notice regarding the cybersecurity event that occurred at our third-party vendor, Infosys McCamish Systems ("IMS") (a subsidiary of Infosys BPM Limited, which is a wholly-owned subsidiary of Infosys Limited). In our initial notification, we identified that this event may have affected the security of certain personal information relating to approximately ninety four (94) Iowa residents that IMS was processing on behalf of our customers. As the investigation continued, one (1) additional Iowa resident was identified as impacted by the event at IMS and the notice is being mailed to this individual on March 15, 2024, via U.S. Mail. A copy of our notification template is enclosed as **Attachment A**. The total number of Iowa residents impacted at the event at IMS is ninety five (95).

We remain engaged with IMS as they continue their investigation and review of this incident and its impact on the data they maintain for us and we will provide your office with updates as appropriate.

Respectfully,

Brian Leary
Chief Compliance Officer

Fidelity Investments Life Insurance Company
Empire Fidelity Investments Life Insurance Company

ATTACHMENT A

<Date Mailed>

<First Name><Last Name>
<Address Line 1>
<Address Line 2>
<City>, <State> <Zip>

Notice of Data Breach

Dear <First Name> <Last Name>,

Fidelity Investments Life Insurance Company ("FILI") is notifying you of a cybersecurity event that has occurred at Infosys McCamish, LLC ("IMS"), a third-party service provider we use in the administration of your FILI life insurance policy. The incident likely resulted in an unauthorized third party obtaining information held by IMS regarding you and your policy. We are writing to provide you with information about this event, and some additional measures you can take to help you protect against possible identity theft or fraud.

WHAT HAPPENED?
In early November, IMS notified us that it experienced a cybersecurity event which disrupted the services that IMS provides for us. Since learning of this event, we have been engaged with IMS to understand IMS's actions to investigate and contain the event, implement remedial measures, and safely restore its services. In response to the incident, IMS retained a third party firm which conducted a forensics investigation of the incident. Through that investigation, IMS learned that between October 29, 2023, and November 2, 2023, an unauthorized third party gained access to certain IMS systems and obtained data stored on those systems. We believe it is likely that the data included certain information about you, as further described below. Please note that this incident did not impact or involve any of FILI's networks or systems.

WHAT INFORMATION WAS INVOLVED?
IMS continues to investigate and review the incident. At this point, they are unable to determine with certainty what personal information was accessed as a result of this incident. However, based on information recently provided by IMS to FILI, we believe that the following information related to you was likely acquired by the third party: your name, Social Security number, state of residence, bank account and routing number (if you provided that information to us to make premium payments on your life insurance policy) and date of birth.

WHAT WE ARE DOING.
We take this event and the security of personal information in our care and in the care of our vendors very seriously. As noted above, upon learning of this incident, we quickly engaged with IMS to understand the nature and scope of the incident and determine the impact on FILI and its customers. Once IMS provided indication that data about some FILI customers may have been exfiltrated by the third party, we conducted a manual review of our records to identify the individuals potentially affected by this event. In addition, we remain engaged with IMS as they continue their investigation of this incident and its impact on the data they maintain for FILI.

WHAT YOU CAN DO.
While we are not aware of any misuse of your personal information because of this incident**, we have arranged for you to enroll, at your option, in credit monitoring and identity restoration services for 24 months at no cost to you.** This service allows you to monitor your credit reports and to detect any unusual activity that may affect your personal financial situation. The service is provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies. If you decide to enroll, please refer to the enclosed instruction sheet.

We encourage you to remain vigilant for fraudulent activity or identity theft by regularly reviewing your statements for your financial and other accounts, monitoring your credit reports, and promptly reporting any suspicious activity to local law enforcement, or your appropriate state authority. For details on additional ways to protect yourself, please refer to the enclosed instruction sheet.

FOR MORE INFORMATION.
If you have additional questions regarding this incident, please feel free to call us at (844) 528-1268, Monday through Friday from 8:30 am to 7:00 pm ET.

If you need assistance with the credit monitoring and identity restoration services offered through TransUnion, please call TransUnion at 1-855-288-5422, Monday through Friday from 8:00 am to 9:00 pm ET, and Saturday and Sunday from 8:00 am to 5:00 pm ET.

We take the protection of customer information very seriously and sincerely apologize for any concern or inconvenience this may have caused.

Sincerely,

Chintan Parekh

Chief Privacy Officer

COMPLIMENTARY CREDIT MONITORING AND IDENTITY THEFT RESTORATION SERVICES INSTRUCTIONS

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service for 2-years provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in this service, go directly to the website at https://bfs.cyberscout.com/activate and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code **<Credit Monitoring Code>** and follow the 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 following 6-digit telephone pass code [redacted] 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 **June 30, 2024**. 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®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain 2-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, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Certain policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the myTrueIdentity Customer Service Team toll-free at: **1-844-787-4607**, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

ADDITIONAL STEPS TO PROTECT YOURSELF

Directions for Placing a Fraud Alert:
You may want to consider placing an initial fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies. The agency that processes your fraud alert will notify the other two credit reporting agencies on your behalf. An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit reporting companies. Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), full name and employer(s). Notify the credit reporting companies if any information is incorrect.

Equifax: 877-478-7625 www.equifax.com; PO Box 740241, Atlanta GA, 30374-0241
Experian: 888-397-3742 www.experian.com; PO Box 9532, Allen TX 75013
TransUnion LLC: 800-680-7289 www.transunion.com; PO Box 6790, Fullerton CA 92834

Directions for Obtaining a Credit Report
Please remember that while this matter may not involve significant risk, it is always good practice to take sensible steps to protect yourself by regularly reviewing your account statements and your credit report. As you may know, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the major credit reporting agencies. You may obtain a free copy of your credit report by calling 1-877-FACT ACT (1-877-322-8228) or by visiting www.annualcreditreport.com.

Resources
Additional information on identity theft is available from the Federal Trade Commission (FTC). You may contact the FTC to report any incidents of identity theft and to obtain guidance about protecting against identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
Toll-free Identity Theft Helpline: 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261
Website: www.ftc.gov/bcp/edu/microsites/idtheft/

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately 170 Rhode Island residents that may be impacted by this event.

<Date Mailed>

<First Name><Last Name>
<Address Line 1><Address Line 2>
<City>, <State> <Zip>

Notice of Data Breach

Dear <First Name> <Last Name>,

Empire Fidelity Investments Life Insurance Company ("EFILI") is notifying you of a cybersecurity event that has occurred at Infosys McCamish, LLC ("IMS"), a third-party service provider we use in the administration of your EFILI life insurance policy. The incident likely resulted in an unauthorized third party obtaining information held by IMS regarding you and your policy. We are writing to provide you with information about this event, and some additional measures you can take to help you protect against possible identity theft or fraud.

WHAT HAPPENED?
In early November, IMS notified us that it experienced a cybersecurity event which disrupted the services that IMS provides for us. Since learning of this event, we have been engaged with IMS to understand IMS's actions to investigate and contain the event, implement remedial measures, and safely restore its services. In response to the incident, IMS retained a third party firm which conducted a forensics investigation of the incident. Through that investigation, IMS learned that between October 29, 2023, and November 2, 2023, an unauthorized third party gained access to certain IMS systems and obtained data stored on those systems. We believe it is likely that the data included certain information about you, as further described below. Please note that this incident did not impact or involve any of EFILI's networks or systems.

WHAT INFORMATION WAS INVOLVED?
IMS continues to investigate and review the incident. At this point, they are unable to determine with certainty what personal information was accessed as a result of this incident. However, based on information recently provided by IMS to EFILI, we believe that the following information related to you was likely acquired by the third party: your name, Social Security number, state of residence, bank account and routing number (if you provided that information to us to make premium payments on your life insurance policy) and date of birth.

WHAT WE ARE DOING.
We take this event and the security of personal information in our care and in the care of our vendors very seriously. As noted above, upon learning of this incident, we quickly engaged with IMS to understand the nature and scope of the incident and determine the impact on EFILI and its customers. Once IMS provided indication that data about some EFILI customers may have been exfiltrated by the third party, we conducted a manual review of our records to identify the individuals potentially affected by this event. In addition, we remain engaged with IMS as they continue their investigation of this incident and its impact on the data they maintain for EFILI.

WHAT YOU CAN DO.
While we are not aware of any misuse of your personal information because of this incident**, we have arranged for you to enroll, at your option, in credit monitoring and identity restoration services for 24 months at no cost to you.** This service allows you to monitor your credit reports and to detect any unusual activity that may affect your personal financial situation. The service is provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies. If you decide to enroll, please refer to the enclosed instruction sheet.

We encourage you to remain vigilant for fraudulent activity or identity theft by regularly reviewing your statements for your financial and other accounts, monitoring your credit reports, and promptly reporting any suspicious activity to local law enforcement, or your appropriate state authority. For details on additional ways to protect yourself, please refer to the enclosed instruction sheet.

FOR MORE INFORMATION.
If you have additional questions regarding this incident, please feel free to call us at (844) 528-1268, Monday through Friday from 8:30 am to 7:00 pm ET.

If you need assistance with the credit monitoring and identity restoration services offered through TransUnion, please call TransUnion at (844)-787-4607, Monday through Friday from 8:00 am to 9:00 pm ET, and Saturday and Sunday from 8:00 am to 5:00 pm ET.

We take the protection of customer information very seriously and sincerely apologize for any concern or inconvenience this may have caused.

Sincerely,

Chintan Parekh

Chief Privacy Officer

COMPLIMENTARY CREDIT MONITORING AND IDENTITY THEFT RESTORATION SERVICES INSTRUCTIONS

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (myTrueIdentity) for 2-years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the website at https://bfs.cyberscout.com/activate and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code **<Credit Monitoring Code>** and follow the 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 following 6-digit telephone pass code [redacted] 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 **June 30, 2024**. 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®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain 2-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, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Certain policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the myTrueIdentity Customer Service Team toll-free at: **1-844-787-4607**, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

ADDITIONAL STEPS TO PROTECT YOURSELF

Directions for Placing a Fraud Alert:
You may want to consider placing an initial fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies. The agency that processes your fraud alert will notify the other two credit reporting agencies on your behalf. An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit reporting companies. Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), full name and employer(s). Notify the credit reporting companies if any information is incorrect.

Equifax: 877-478-7625 www.equifax.com; PO Box 740241, Atlanta GA, 30374-0241
Experian: 888-397-3742 www.experian.com; PO Box 9532, Allen TX 75013
TransUnion LLC: 800-680-7289 www.transunion.com; PO Box 6790, Fullerton CA 92834

Directions for Obtaining a Credit Report
Please remember that while this matter may not involve significant risk, it is always good practice to take sensible steps to protect yourself by regularly reviewing your account statements and your credit report. As you may know, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the major credit reporting agencies. You may obtain a free copy of your credit report by calling 1-877-FACT ACT (1-877-322-8228) or by visiting www.annualcreditreport.com.

Resources
Additional information on identity theft is available from the Federal Trade Commission (FTC). You may contact the FTC to report any incidents of identity theft and to obtain guidance about protecting against identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
Toll-free Identity Theft Helpline: 1-877-ID-THEFT (1-877-438-4338); TTY: 1 866-653-4261
Website: www.ftc.gov/bcp/edu/microsites/idtheft/

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately 170 Rhode Island residents that may be impacted by this event.

<Date Mailed>

<First Name><Last Name>
<Address Line 1>
<Address Line 2>
<City>, <State> <Zip>

Notice of Data Breach

Dear <First Name><Last Name>,

Fidelity Investments Life Insurance Company ("FILI") is notifying you of a cybersecurity event that has occurred at Infosys McCamish, LLC ("IMS"), a third-party service provider we use in the administration of certain FILI life insurance policies. The incident likely resulted in an unauthorized third-party obtaining certain personal information about you (details of which are provided below) that was held by IMS. We had received your personal information from the holder of a policy that we issued. We are writing to provide you with information about this event, and some additional measures you can take to help you protect against possible identity theft or fraud.

WHAT HAPPENED?
In early November, IMS notified us that it experienced a cybersecurity event which disrupted the services that IMS provides for us. Since learning of this event, we have been engaged with IMS to understand IMS's actions to investigate and contain the event, implement remedial measures, and safely restore its services. In response to the incident, IMS retained a third party firm which conducted a forensics investigation of the incident. Through that investigation, IMS learned that between October 29, 2023, and November 2, 2023, an unauthorized third party gained access to certain IMS systems and obtained data stored on those systems. We believe it is likely that the data included certain information about you, as further described below. Please note that this incident did not impact or involve any of FILI's networks or systems.

WHAT INFORMATION WAS INVOLVED?
IMS continues to investigate and review the incident. At this point, they are unable to determine with certainty what personal information was accessed as a result of this incident. However, based on information recently provided by IMS to EFILI, we believe that the following information related to you was likely acquired by the third party: your name, Social Security number and, if provided by the policy holder, your address.

WHAT WE ARE DOING.
We take this event and the security of personal information in our care and in the care of our vendors very seriously. As noted above, upon learning of this incident, we quickly engaged with IMS to understand the nature and scope of the incident and determine the impact on FILI and its customers. Once IMS provided indication that data about some FILI policies may have been exfiltrated by the third party, we conducted a manual review of our records to identify the individuals potentially affected by this event. In addition, we remain engaged with IMS as they continue their investigation of this incident and its impact on the data they maintain for FILI.

WHAT YOU CAN DO.
While we are not aware of any misuse of your personal information because of this incident**, we have arranged for you to enroll, at your option, in credit monitoring and identity restoration services for 24 months at no cost to you.** This service allows you to monitor your credit reports and to detect any unusual activity that may affect your personal financial situation. The service is provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies. If you decide to enroll, please refer to the enclosed instruction sheet.

We encourage you to remain vigilant for fraudulent activity or identity theft by regularly reviewing your statements for your financial and other accounts, monitoring your credit reports, and promptly reporting any suspicious activity to local law enforcement, or your appropriate state authority. For details on additional ways to protect yourself, please refer to the enclosed instruction sheet.

FOR MORE INFORMATION.
If you have additional questions regarding this incident, please feel free to call us at (844) 528-1268, Monday through Friday from 8:30 am to 7:00 pm ET.

If you need assistance with the credit monitoring and identity restoration services offered through TransUnion, please call TransUnion at 1-855-288-5422, Monday through Friday from 8:00 am to 9:00 pm ET, and Saturday and Sunday from 8:00 am to 5:00 pm ET.

We take the protection of personal information very seriously and sincerely apologize for any concern or inconvenience this may have caused.

Sincerely,

Chintan Parekh

Chief Privacy Officer

COMPLIMENTARY CREDIT MONITORING AND IDENTITY THEFT RESTORATION SERVICES INSTRUCTIONS

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service for 2-years provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in this service, go directly to the website at https://bfs.cyberscout.com/activate and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code **<Credit Monitoring Code>** and follow the 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 following 6-digit telephone pass code [redacted] 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 **June 30, 2024**. 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®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain 2-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, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Certain policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the myTrueIdentity Customer Service Team toll-free at: **1-844-787-4607**, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

ADDITIONAL STEPS TO PROTECT YOURSELF

Directions for Placing a Fraud Alert:
You may want to consider placing an initial fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies. The agency that processes your fraud alert will notify the other two credit reporting agencies on your behalf. An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit reporting companies. Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), full name and employer(s). Notify the credit reporting companies if any information is incorrect.

Equifax: 877-478-7625 www.equifax.com; PO Box 740241, Atlanta GA, 30374-0241
Experian: 888-397-3742 www.experian.com; PO Box 9532, Allen TX 75013
TransUnion LLC: 800-680-7289 www.transunion.com; PO Box 6790, Fullerton CA 92834

Directions for Obtaining a Credit Report
Please remember that while this matter may not involve significant risk, it is always good practice to take sensible steps to protect yourself by regularly reviewing your account statements and your credit report. As you may know, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the major credit reporting agencies. You may obtain a free copy of your credit report by calling 1-877-FACT ACT (1-877-322-8228) or by visiting www.annualcreditreport.com.

Resources
Additional information on identity theft is available from the Federal Trade Commission (FTC). You may contact the FTC to report any incidents of identity theft and to obtain guidance about protecting against identity theft.

Federal Trade Commission
Consumer Response Center 600
Pennsylvania Avenue, NW
Washington, DC 20580
Toll-free Identity Theft Helpline: 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261 Website:
www.ftc.gov/bcp/edu/microsites/idtheft/

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately 184 Rhode Island residents that may be impacted by this event.

<Date Mailed>

<First Name><Last Name>
<Address Line 1><Address Line 2>
<City>, <State> <Zip>

Notice of Data Breach

Dear <First Name><Last Name>,

Empire Fidelity Investments Life Insurance Company ("EFILI") is notifying you of a cybersecurity event that has occurred at Infosys McCamish, LLC ("IMS"), a third-party service provider we use in the administration of certain EFILI life insurance policies. The incident likely resulted in an unauthorized third-party obtaining certain personal information about you (details of which are provided below) that was held by IMS. We had received your personal information from the holder of a policy that we issued. We are writing to provide you with information about this event, and some additional measures you can take to help you protect against possible identity theft or fraud.

WHAT HAPPENED?
In early November, IMS notified us that it experienced a cybersecurity event which disrupted the services that IMS provides for us. Since learning of this event, we have been engaged with IMS to understand IMS's actions to investigate and contain the event, implement remedial measures, and safely restore its services. In response to the incident, IMS retained a third party firm which conducted a forensics investigation of the incident. Through that investigation, IMS learned that between October 29, 2023, and November 2, 2023, an unauthorized third party gained access to certain IMS systems and obtained data stored on those systems. We believe it is likely that the data included certain information about you, as further described below. Please note that this incident did not impact or involve any of EFILI's networks or systems.

WHAT INFORMATION WAS INVOLVED?
IMS continues to investigate and review the incident. At this point, they are unable to determine with certainty what personal information was accessed as a result of this incident. However, based on information recently provided by IMS to EFILI, we believe that the following information related to you was likely acquired by the third party: your name, Social Security number and, if provided by the policy holder, your address.

WHAT WE ARE DOING.
We take this event and the security of personal information in our care and in the care of our vendors very seriously. As noted above, upon learning of this incident, we quickly engaged with IMS to understand the nature and scope of the incident and determine the impact on EFILI and its customers. Once IMS provided indication that data about some EFILI policies may have been exfiltrated by the third party, we conducted a manual review of our records to identify the individuals potentially affected by this event. In addition, we remain engaged with IMS as they continue their investigation of this incident and its impact on the data they maintain for EFILI.

WHAT YOU CAN DO.
While we are not aware of any misuse of your personal information because of this incident**, we have arranged for you to enroll, at your option, in credit monitoring and identity restoration services for 24 months at no cost to you.** This service allows you to monitor your credit reports and to detect any unusual activity that may affect your personal financial situation. The service is provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies. If you decide to enroll, please refer to the enclosed instruction sheet.

We encourage you to remain vigilant for fraudulent activity or identity theft by regularly reviewing your statements for your financial and other accounts, monitoring your credit reports, and promptly reporting any suspicious activity to local law enforcement, or your appropriate state authority. For details on additional ways to protect yourself, please refer to the enclosed instruction sheet.

FOR MORE INFORMATION.
If you have additional questions regarding this incident, please feel free to call us at (844) 528-1268, Monday through Friday from 8:30 am to 7:00 pm ET.

If you need assistance with the credit monitoring and identity restoration services offered through TransUnion, please call TransUnion at (844)-787-4607, Monday through Friday from 8:00 am to 9:00 pm ET, and Saturday and Sunday from 8:00 am to 5:00 pm ET.

We take the protection of personal information very seriously and sincerely apologize for any concern or inconvenience this may have caused.

Sincerely,

Chintan Parekh

Chief Privacy Officer

COMPLIMENTARY CREDIT MONITORING AND IDENTITY THEFT RESTORATION SERVICES INSTRUCTIONS

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online three-bureau credit monitoring service (myTrueIdentity) for 2-years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the website at https://bfs.cyberscout.com/activate and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code **<Credit Monitoring Code>** and follow the 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 following 6-digit telephone pass code [redacted] 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 **June 30, 2024**. 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®, Experian® and Equifax®, or an address in the United States (or its territories) and a valid Social Security number or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain 2-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, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Certain policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the myTrueIdentity Customer Service Team toll-free at: **1-844-787-4607**, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

ADDITIONAL STEPS TO PROTECT YOURSELF

Directions for Placing a Fraud Alert:
You may want to consider placing an initial fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies. The agency that processes your fraud alert will notify the other two credit reporting agencies on your behalf. An initial fraud alert stays on your credit report for 90 days. When you place this alert on your credit report, you will receive information about ordering one free credit report from each of the credit reporting companies. Once you receive your reports, review them carefully for inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain. Verify the accuracy of your Social Security number, address(es), full name and employer(s). Notify the credit reporting companies if any information is incorrect.

Equifax: 877-478-7625 www.equifax.com; PO Box 740241, Atlanta GA, 30374-0241
Experian: 888-397-3742 www.experian.com; PO Box 9532, Allen TX 75013
TransUnion LLC: 800-680-7289 www.transunion.com; PO Box 6790, Fullerton CA 92834

Directions for Obtaining a Credit Report
Please remember that while this matter may not involve significant risk, it is always good practice to take sensible steps to protect yourself by regularly reviewing your account statements and your credit report. As you may know, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the major credit reporting agencies. You may obtain a free copy of your credit report by calling 1-877-FACT ACT (1-877-322-8228) or by visiting www.annualcreditreport.com.

Resources
Additional information on identity theft is available from the Federal Trade Commission (FTC). You may contact the FTC to report any incidents of identity theft and to obtain guidance about protecting against identity theft.

Federal Trade Commission
Consumer Response Center 600
Pennsylvania Avenue, NW
Washington, DC 20580
Toll-free Identity Theft Helpline: 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261
Website: www.ftc.gov/bcp/edu/microsites/idtheft/

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

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

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately 184 Rhode Island residents that may be impacted by this event.